NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE ECONOMIC AND RISK CONSTRAINTS IN THE FEASIBILITY ANALYSIS OF WIRELESS COMMUNICATIONS IN MARINE CORPS COMBAT OPERATION CENTERS

by

William L. Travis

September 2013

Thesis Advisor: Alex Bordetsky
Second Reader: Glen Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE THE ECONOMIC AND RISK CONSTRAINTS IN THE FEASIBILITY ANALYSIS OF WIRELESS COMMUNICATIONS IN MARINE CORPS COMBAT OPERATION CENTERS			**5. FUNDING NUMBERS**
6. AUTHOR(S) William L. Travis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis will provide Marine Corps acquisitions and communications personnel a general understanding of wireless communications capabilities, financial feasibility, benefits and the risks of implementing a wireless solution into the current existing communications infrastructure in particular, the Combat Operations Center (COC) CapSet models already employed and deployed throughout the Marine Corps Air Ground Task Force. The content of this thesis is of an unclassified nature. This thesis is intended to serve as a reference for acquisitions or communications personnel dealing with the acquisition, procurement, planning, and implementation of wireless technologies in the Marine Corps, so that they will be able to intelligently articulate the financial feasibility, benefits, and risks of adopting or implementing a wireless solution to the Marine Corps Enterprise Network and COC infrastructure, and make informed decisions on the subject.

14. SUBJECT TERMS IT, Wi-Fi, Marine Corps, COC CapSets, Wireless, Budgets			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE ECONOMIC AND RISK CONSTRAINTS IN THE FEASIBILITY ANALYSIS OF WIRELESS COMMUNICATIONS IN MARINE CORPS COMBAT OPERATION CENTERS

William L. Travis
Captain, United States Marine Corps
B.S., Naval Postgraduate School, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: William L. Travis

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Glen Cook
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will provide Marine Corps acquisitions and communications personnel a general understanding of wireless communications capabilities, financial feasibility, benefits and the risks of implementing a wireless solution into the current existing communications infrastructure in particular, the Combat Operations Center (COC) CapSet models already employed and deployed throughout the Marine Corps Air Ground Task Force. The content of this thesis is of an unclassified nature. This thesis is intended to serve as a reference for acquisitions or communications personnel dealing with the acquisition, procurement, planning, and implementation of wireless technologies in the Marine Corps, so that they will be able to intelligently articulate the financial feasibility, benefits, and risks of adopting or implementing a wireless solution to the Marine Corps Enterprise Network and COC infrastructure, and make informed decisions on the subject.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AO	Area of Operations
AP	Access Point
CapSet	Capability Set
COC	Command Operations Center
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DAA	Designated Accrediting Authority
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
RF	Radio Frequency
IEEE	Institute of Electrical and Electronics Engineers
IA	Information Assurance
IAED	Information Assurance Enterprise Directive
IP	Internet Protocol
IT	Information Technology
KM	Knowledge Management
LAN	Local Area Network
MAGTF	Marine Air Ground Task Force
MANET	Mobile Ad-hoc Network
MCEN	Marine Corps Enterprise Network
MCNOSC	Marine Corps Network Operations and Security Command
MCS	MAGTF Communications Systems
MCTSSA	Marine Corps Tactical Systems Support Activity
MSC	Major Subordinate Command

NECC	Net-Enabled Command Capability
NCW	Network Centric Warfare
NIPRNet	Non-Secure Internet Protocol Router Network
NLOS	Non-Line of Sight
NOC	Network Operations Center
NOTM	Network On-the-Move
OCO	Overseas Contingency Operations
ODFM	Orthogonal Frequency Division Multiplexing
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
OTM	On-the-Move
P2P	Peer-to-Peer
P2MP	Peer-to-Multi-Peer
PTP	Point-to-Point
RF	Radio Frequency
RFC	Request For Comments
SBU	Sensitive But Unclassified
SIPRNet	Secret Internet Protocol Router Network
STEP	Standardized Tactical Entry Point
SWOT	Strengths, Weaknesses, Opportunities, Threats
TDS	Tactical Data Systems
TOC	Tactical Operations Center
UOC	Unit Operations Center
USMC	United States Marine Corps
VLAN	Virtual Local Area Network
WIDS	Wireless Intrusion Detection Systems
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WI-FI	Wireless Fidelity
WIPS	Wireless Internet Protection System
WPAN	Wireless Personal Area Network

ACKNOWLEDGMENTS

I would like to thank all the professors and students in the GSOIS department at the Naval Postgraduate School in Monterey, CA, for their professionalism, knowledge, and support in helping me with this thesis project. I would also like to give special thanks to my thesis advisor, Dr. Bordetsky, for his time, wisdom, and help in creating a graduate-level thesis that may potentially help the Marine Corps organization and/or serve as a reliable reference, or secondary research document, for further exploration research.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In 2010, the Marine Corps released *the Marine Corps War Fighting Publication* (MCWP) 3–40.3, which details the doctrine and procedures for employment of communications systems that enable and support the Marine Air Ground Task Force (MAGTF) on the battlefield. MCWP 3–40.3 (2010) stated that the MAGTF communications system (MCS) needed to satisfy all Command and Control (C2) needs of the expeditionary warfighters and MAGTF echelons on the battlefield. MCWP 3–40.3 (2010) also states that the MAGTF's success in a dynamic and rapidly changing C2 environment, depended on employing a communications system that would satisfy the need for information and "provide MAGTF commanders and their staffs with the tools necessary to collect, process, analyze, and exchange information rapidly in support of operations planning and execution." This MCS capability was to be employed in a manner that would not adversely affect the MAGTF's freedom of action and mobility, in keeping with the Marine Corps communication's doctrine of providing a reliable, flexible, responsive, timely, and configurable communications architecture (MCWP 3–40.3, 2010).

The Marine Corps' previous solution to bridge a gap created by the advancement and constant change of technology, demand, and security in the C2 environment, was the Command Operations Center (COC) Capability Set (CapSet) manufactured by General Dynamics Electronics Division. The COC CapSet is an operations facility utilized at multiple echelons of the MAGTF to execute C2 functions. The CapSet suites are highly mobile and scalable based on the size of the unit and are hardwired with media and communications technology and their own power and transportation trailers. The system supports Sensitive but Unclassified (SBU) IP Data (formerly known as NIPRNET), Secret IP Data (formerly known as SIPRNET), and coalition networks.

A perceived gap in the MCS that exists at the time of the writing of this research paper is the lack of a wireless communications solution that can be securely deployed on

the battlefield or in a tactical environment. Other Department of Defense organizations such as the U.S. Air Force and U.S. Army have already adopted some form of wireless solution in their tactical COCs. The Marine Corps has yet to implement the same wireless communications solution due to possible budgetary and feasibility constraints, the organization's current communications doctrine, equipment and capabilities, or perhaps a lack of understanding and knowledge of 802.11 wireless technologies.

Based upon requests for research proposals from the Marine Corps Systems Command, Marine Corps' units have indicated that wireless capability would be beneficial. However, the Marine Corps' units have not been able to precisely articulate the feasibility, costs, and risks associated with implementing a wireless network in tactical COCs. This is a problem because current and projected budget constraints are likely to reduce the Marine Corps' ability to acquire new Information Technology Systems that will continue to provide the warfighters with the necessary IT capabilities needed to meet the challenges of dynamic operating environments for current and future battlefields.

The purpose of this research is to examine the feasibility, costs, and risks associated with current Marine Corps wired COC networking infrastructures, compared to implementing a new wireless network infrastructure. The analysis of information produced from this research will help Marine Corps Systems Command articulate the strengths, weaknesses, and cost impacts involved with choosing to implement a wireless network solution in the COC. This is important because it will give the Marine Corps Systems Command the information needed to help prioritize its acquisitions efforts and focus on projects that will allow the Marine Corps fleets to continue its competitive dominance in information superiority, despite decreasing resources due to budget constraints.

B. PROBLEM STATEMENT

The problem is the Marine Corps fleet operating forces have identified a need for wireless capabilities in the Command Operations Center but have not been able to precisely articulate the feasibility, costs, and risks associated with implementing a

wireless network. This is a problem because current and projected budget constraints will possibly limit funding for communications equipment, redundant capabilities, and research and development of new alternatives for Command and Control.

C. PURPOSE STATEMENT

The purpose of this research is to examine the feasibility, costs, and risks associated with current Marine Corps COC networking infrastructures, compared to implementing a new wireless network infrastructure. The analysis of information produced from this research will help Marine Corps Systems Command articulate the strengths, weaknesses, requirements, and impacts on costs involved with choosing a new wireless networking infrastructure over the existing wired networking infrastructure. This is important because it will give the Marine Corps Systems Command the information it needs to help prioritize acquisitions efforts and focus decreasing resources (due to budget constraints), on projects that will allow the Marine Corps fleets to continue its competitive dominance in information superiority.

D. LITERATURE REVIEW

Coleman and Westcott's (2012) *Certified Wireless Network Administrator Official Study Guide* is an excellent reference for this research paper because it concentrates on a wide range of essential topics that add to the understanding of wireless 802.11 technology. It covers everything from the fundamentals to the employment of wireless technology. This reference will serve as a key-contributing factor in collecting literature to help build a discussion on important wireless and networking concepts.

Dhawan (2007) examines Bluetooth, WiMAX, and Wi-Fi and examines how these technologies differ from one another. This information can then be presented in a table to allow for the Marine Corps Fleet Commander and acquisition specialists the ability to easily compare and contrast among the different wireless solutions.

There are risks associated with operating a wireless network that differ and/or are not found with hardwired networks. Gast (2005) discusses some of these issues associated with deploying and maintaining wireless networks. For example, Gast (2005)

gives an extensive discussion on wireless security issues such as those occurring with the dynamic WEP standards and information on selecting security protocols. In order for the Marine Corps to implement a wireless network in today's COC, where the operating environment is very dynamic and constantly faced with new emerging threats to information security, Gast's discussion on identifying threats and prevention of these threats are important in articulating the strengths and weaknesses of wireless technology.

Jindal, Jindal, and Gupta (2005) talk about the evolution of the wireless technology and on the different concepts, business models, and configurations of the different wireless communications types. This information can be used to help the researcher understand the subject without having to capture new data. Jindal et al. (2005) cover the benefit of WiMAX technology as "signals running close on wireless channels vice narrow lanes with the capability of utilizing more traffic with fewer disturbances. Many technologies currently available can only provide line of sight (LOS) coverage; the technology behind WI-MAX has been optimized to provide excelled non-line of sight (NLOS) coverage" (Jindal et al., 2005). The WI-MAX technology will be examined to see if it is a feasible solution for a Marine Corps COC.

Currently, the Marine Corps is using the Capability Set (CapSet) Command Operation Centers from General Dynamics. A list of the key components of different CapSets can be analyzed to see if the pre-existing capabilities, such as the system's server and router suite, can be modified to implement a wireless solution and at what cost. It also has pictures that will be helpful in depicting the bulkiness of some of the equipment and the containers they are carried in, which can give the reader a visual of the size and weight of some of this equipment in the COC.

The *Marine Corps Publication on Communications Information Systems*, now known as *The MAGTF Communications System MWCP 3–40.3*, has important information on the doctrine, capabilities, techniques, and concepts behind employing communications resources in the Marine Corps operations. This literature is essential in understanding the needs and requirements of information systems in the Marine Corps and is the basis in accessing the viability and requirements of the current network architecture in order to access the feasibility of alternative wireless solutions.

Rappaport (2006) covers the fundamental issues that affect wireless networks and gives a review on the capabilities and weaknesses of wireless standards and technological developments in the field, such as 3G and Bluetooth technologies. Information on the different wireless technologies can be analyzed and compared to present recommendations to the commander to consider a type of wireless technology that can be used in a Command and Control Operations Center (COC).

Ravichandiran and Vaithiyanathan (2009) give great templates for a table of a SWOT analysis on Wi-Fi, Wi-Fi mesh, and WiMAX technologies along with a comparison of all these wireless technologies. Their information on mesh and WiMAX technologies offer good background information that is included in this thesis paper in order to give the acquisitions personnel and/or communications planner a general understanding of the capabilities, employment, and benefits of these wireless technologies.

Stallings (1998) discusses the risks associated with networking back in the 1990s that are still threats today. This understanding of Network Security is an important subject that needs to be covered in order to properly analyze wireless and hardwired network architectures. Planners, operators, and maintainers of Information Technology must be able to articulate the advantages and disadvantages of these types of IT to their customers. Stallings (1998) does not list costs in his discussion but talks about the type of technology needed such as cryptography algorithm software and other encryption-type software that will be helpful in increasing the knowledge of Marine Corps IT professionals and users.

E. RESEARCH QUESTIONS AND HYPOTHESIS

1. What are the strengths and weaknesses being added by introducing a wireless networking capability to Marine Corps COCs?
2. What are the critical requirements that Marine Corps fleets desire to fulfill by adopting a wireless infrastructure over wired COC capabilities?
3. What are the costs associated with acquiring a wireless capability in comparison to current capabilities and other available options?

4. How long and how well can the Marine Corps continue to operate with current COC capabilities, and what does it gain or lose by adapting a new wireless capability?

F. RESEARCH METHODS

The research for this thesis will be a qualitative study to explore and describe the benefits, issues, costs, and risk constraints for the Marine Corps to implement a wireless capability over its existing wired capability. The information and data collected will primarily come from previous research and studies of similar topics on the subject. Data will be captured by also researching other military agencies that currently use wireless communications in their command centers. All the information and data collected will be of an unclassified nature, and can be acquired from unclassified sources found in the library, acquisition documents, secondary research, and online. This research will not involve any lab work but may require travel if needed to interview other services' communications personnel for interviews.

G. PROPOSED DATA, OBSERVATION, AND ANALYSIS METHODS

Statistical methods will be used in order to help summarize, describe, and compare collected data. Previous research and documents will be used to analyze and interpret the data to help articulate to the intended audience a better understanding of complex information if said audience is not familiar with the Information Sciences.

H. POTENTIAL BENEFITS, LIMITATIONS, RECOMMENDATIONS

The potential benefit that may result from this thesis study is, to gain a better understanding of the problem area within the Marine Corps' decision whether or not to adopt a new wireless technology or keep their current technology in the COC. This research will also give decision-makers the ability to articulate the feasibility of adopting wireless communications along with the weaknesses and risks associated with this technology. This research can also serve as an information source to help decision makers make informed decisions in their acquisition process. Limitations to this thesis study are due to time constraints on the researcher's ability to collect data, prepare, and complete

this research. A recommendation for this thesis study is to use updated costs to produce a cost based analysis in order to compare advantages and disadvantages to adopting a wireless infrastructure or keeping the current wired infrastructure.

I. CHAPTER OUTLINE

This thesis report is organized into five chapters.

Chapter I provide an introduction to the problem and purpose of this research and a discussion of the literature referenced in this research.

Chapter II discusses the background and overview of wireless networking technology.

Chapter III is a discussion of the current Marine Corps COC's capabilities, guidance, and analysis of budget constraints that affect the Marine Corps acquisition and procurement ability.

Chapter IV examines the economics and provides a SWOT and comparative analysis of current COC capabilities and wireless technology solutions available.

Chapter V summarizes the information discussed in the previous chapters and concludes with recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND AND OVERVIEW OF WIRELESS NETWORKING TECHNOLOGY

A. BACKGROUND

The purpose of this chapter is to provide a general understanding of the background, fundamentals, standards and organizations, capabilities, and strengths and weaknesses of Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless to acquisitions and communications personnel and other key stakeholders involved with the decision-making in acquiring IT systems for the Marine Corps. IEEE 802.11 wireless is a standard for providing local area network (LAN) communications using radio frequencies (Coleman & Westcott, 2012).

The concept of communicating by transferring information between two unconnected points is not new by any means. The United States Military first used communication using wireless technologies during World War II to relay battle plans back and forth between enemy and friendly lines (Coleman & Westcott, 2012). One of the first wireless networks developed was the ALOHAnet (Coleman & Westcott, 2012). The ALOHAnet used a wireless shared medium in the 400 MHZ frequency range to communicate between the Hawaiian Islands across a LAN communication Open Systems Interconnection (OSI) layer 2 protocols called ALOHA (Coleman & Westcott). The development of the ALOHAnet at the University of Hawaii in late 1960s and early 1970s provides historical insight into a range of wireless data network applications at the start of the 21st century (Schwartz & Abramson, 2009). It was not until the 1990s that commercial wireless networking vendors started making low-speed wireless data networking products, such as mobile phones, across the 900 MHz frequency band (Coleman & Westcott, 2012).

In 1991, the IEEE began discussions for standardizing wireless local area network (WLAN) technologies, finally ratifying the original legacy 802.11 wireless network standards forming the building blocks for WLAN technology (Coleman & Westcott). When wireless technology was deployed to businesses and corporations between 1997 and 1999, there was initial resistance before these entities, as well as home users, soon

began to realize the benefits and potential of having wireless networking (Coleman & Westcott, 2012). Today vendors such as Apple, which makes the iPhone and iPad, have helped revolutionize the IT world with their wireless data networking products. The demand for wireless technology has increased so drastically in the past five years that the market has now become saturated with wireless devices (PricewaterhouseCoopers, 2013).

Today, IEEE 802.11 wireless networks are more commonly referred to as Wi-Fi, the brand name created by the industry, and used to market WLAN technology (Coleman & Westcott, 2012). You can now find WLAN technology implemented and used in almost every home and office in the United States and other countries. Some common products that use this technology today are mobile phones, hand-held radios, laptops, computer peripherals, remote control cars, as well as thousands of other devices. The popularity and need for wireless networking solutions has increased as a result of the change in emphasis toward mobile systems and technology, which has become particularly popular and important to the younger and middle-age populations across the globe. Figure 1 shows a picture of a simple wireless networking architecture.

Figure 1. Wireless network picture (From Brain et al., 2013)

B. WIRELESS FUNDAMENTAL KNOWLEDGE

Budget constraints and cutbacks are affecting the decisions of numerous organizations throughout the DoD. In 2010 Lieutenant General George Flynn, commanding general of the Marine Corps Combat Development Command, stated that the Marine Corps needed to balance investments between current and future challenges (Jean, 2010). The difference in investment dollars well spent and lost can come down to the IT acquisitions personnel's fundamental knowledge of wireless technologies when contracting with the right vendor to make the right product. Many bad contracts and obligations are made due to acquisitions officers not knowing what they are buying when it comes to IT. In order to make better decisions in the acquisition or non-acquisition of wireless technologies, it is important that the key stakeholders possess a fundamental knowledge and understanding of IEEE 802.11 wireless technology. This section is dedicated to building a basic understanding of some fundamental elements in wireless communications and technology.

1. The OSI Model

The cornerstone of data communications is the Open Systems Interconnection (OSI) model (Coleman & Westcott, 2012). The OSI model is a conceptual model developed by the International Organization for Standardization (ISO) in 1984 and is made up of seven layers as shown in Table 1 (Voelcker, 1986). Each layer utilizes the services of the layers underneath (Coleman & Westcott, 2012).

Layer 7	Application	Http, SMTP,SNMP
Layer 6	Presentation	MIME, XDR
Layer 5	Session	SOCKS, TLS/SSL
Layer 4	Transport	TCP, UDP
Layer 3	Network	IP, Apple Talk
Layer 2	Data – Link	IEEE 802.2, 802.3
Layer 1	Physical	IEEE 802.11, Bluetooth

Table 1. OSI Model (After Coleman & Westcott, 2012)

Layer 1, also known as the physical layer, is the lowest level of the OSI model and includes the functions needed to activate, maintain, and deactivate physical connections (Coleman & Westcott, 2012). This layer defines functional and procedural characteristics of the interface to the physical circuit (Coleman & Westcott, 2012). Voelcker (1986) states "the electrical and mechanical specifications are considered to be part of the medium itself." An example of layer 1 technology is IEEE 802.3 standard for category 5 (CAT-5) Ethernet cable (Shirey, 2012).

Layer 2, also known as the data – link layer, is responsible for the synchronization and error processing for information transmitted over the physical link (Coleman & Westcott, 2012).

Layer 3, also known as the network layer, is responsible for routing communications through network resources to the system where the communicating application resides; fragment segmentation and reassembly of data packets and some error correction is done at this layer (Coleman & Westcott, 2012).

Layer 4, also known as the transport layer, is responsible for the reliable end-to-end transportation of data (Coleman & Westcott, 2012). It also includes functions like multiplexing multiple independent message streams over a single connection and segmenting data into appropriately sized units for the network layer (Coleman & Westcott, 2012).

Layer 5, also known as the session layer, the functions our analogous to the control language used to run a computer system (Coleman & Westcott, 2012). The session layer begins, manages, and terminates the session between a local and remote application (Coleman & Westcott, 2012).

Layer 6, also known as the presentation layer, ensures that information delivered between two systems can understand each other by translating the communicating machines' syntax if needed (Coleman & Westcott, 2012).

Layer 7, the application layer, manipulates information in order to support distributed applications (Coleman & Westcott, 2012). This layer allows the user to interact directly with software applications and provides widest variety of work being done on the OSI layers (Coleman & Westcott, 2012). Figure 2 depicts both the OSI model and IEEE 802.11 wireless.

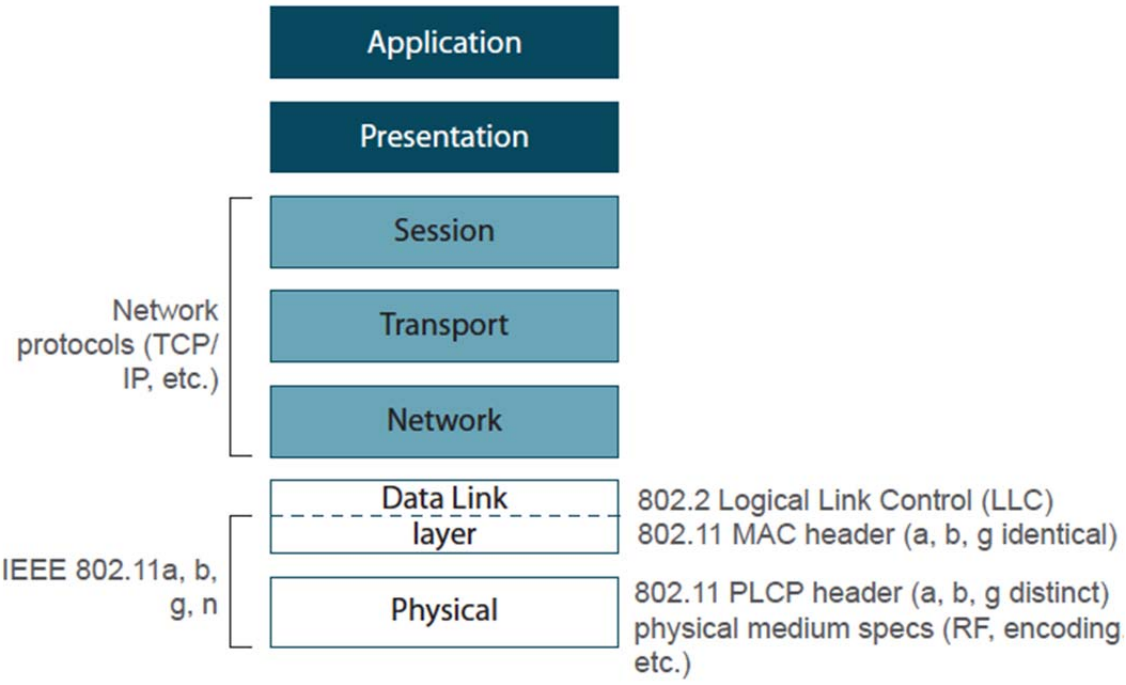

Figure 2. OSI Model and 802.11 (From Wild Packets, n.d.)

IEEE 802.11 wireless technologies use layers 1 and 2 (Coleman & Westcott, 2012). In a wired network infrastructure, radio frequency (RF) signals and data in binary form (1s and 0s) move across physical wires such as copper cables, CAT-5, and fiber optic cables (Coleman & Westcott, 2012). Wireless network infrastructures are opposite, in that RF signals and data move through the atmosphere, hence the term "wireless" (Coleman & Westcott, 2012). Coleman and Westcott ask some important questions that acquisitions specialists and communications planners and installers should be aware of or provide general solutions that will mitigate the effects of risks when dealing with this technology.

> Why does a wireless network perform differently in an auditorium full of people than it does inside an empty auditorium? Why does the performance of a wireless LAN seems to degrade in a storage area with metal racks? Why does the range of a 5 GHz radio transmitter seem shorter than the range of a 2.4 GHz radio card? (Coleman & Westcott, 2012)

Answers to the aforementioned questions could prove to be vital to the decisions that acquisitions specialists and communications planners and users make when choosing the best qualified vendor that can provide the best wireless technology solution that fits within the organizations' initial capabilities document (ICD), specifications, and fiscal constraints. It may also come in good use to that communications planner tasked with providing wireless communications services to multiple users either confined in close proximity and/or spread out across their operating environment.

2. Radio Frequency Components and Operation

The key components in the creation of a wireless medium are the transmitter, antenna, and receiver (Coleman & Westcott, 2012). When the computer sends the data to the transmitter, the transmitter then initiates the RF communication by generating an alternating current (AC) signal, determining the frequency of the transmission and then transporting the data directly to the antenna (Coleman & Westcott, 2012). The antenna collects the AC signal from the transmitter and then radiates or directs those RF waves away from the antenna to the receiver (Coleman & Westcott, 2012). The receiver takes

this signal, called the carrier signal, translates the signal into 1s and 0s, and then passes this data to the computer to be processed (Coleman & Westcott, 2012).

3. Radio Frequency Signal Characteristics

The electromagnetic spectrum is the range of self-propagating electromagnetic waves that have the ability to transverse across and through both matter and space (Coleman & Westcott, 2012). Antennas are used to radiate the RF electromagnetic signal away from it in a continuous pattern governed by radio frequency characteristics defined by the laws of physics, wavelength, frequency, amplitude, and phase (Coleman & Westcott, 2012). Coleman and Westcott (2012) define wavelength simply as the distance traveled by a single cycle of an RF signal. They describe frequency as "the number of times a specified event occurs within a specified time interval" (Coleman & Westcott, 2012). Amplitude is the signal's strength, "when speaking about wireless transmissions, this is often referenced as how loud or strong the signal is" (Coleman & Westcott, 2012). Finally the phase involves the relationship between two more signals when they share the same frequency (Coleman & Westcott, 2012).

Coleman and Westcott (2012) state that

> It is very important to understand that there is an inverse relationship between wavelength and frequency. The three components of this inverse relationship are frequency (measured in hertz), wavelength (measured in meters), and speed of light. The larger the wavelength of an RF signal, the lower the frequency of that signal and the higher the frequency of an RF signal, the smaller the wavelength.

4. How Radio Frequencies Behave

RF signals move and behave in different manners when it travels either through wired mediums or wirelessly (Coleman & Westcott, 2012). The ways these signals move are known as wave propagation (Coleman & Westcott, 2012). The different types of RF wave propagation behaviors, which explain what happens to that signal as it moves from one location to the next, are absorption, reflection, scattering, refraction, diffraction, and multipath (Coleman & Westcott, 2012). It is important to understand these RF propagation behaviors because it will allow for better decision-making in the acquisition

of wireless products when examining equipment capabilities, as well as aid planners in the proper installation and employment of wireless technologies (Coleman & Westcott, 2012).

The first and most common type of RF wave propagation behavior to be discussed is absorption. Absorption occurs when a signal is absorbed or stopped by an object such as a large body of water, brick or concrete walls, along its path (Coleman & Westcott, 2012). Absorption is the leading and most common cause of decreased signal strength or amplitude, called signal attenuation or loss (Coleman & Westcott, 2012). The increase of signal strength is referred to as gain, or amplification. An example of absorption that occurs, which planners often neglect to consider, is when wireless access points (AP) are installed in large occupied conference rooms, the signal can be absorbed by the collection of water in the human body, which averages between 50 and 60 percent (Coleman & Westcott, 2012). As an added note, APs installed in large conference rooms may also experience effects of degraded signal strength because of lack of available bandwidth (Coleman & Westcott, 2012).

When installing wireless APs, the planner should also be aware of the RF propagation behavior called reflection. Reflection occurs when the signal encounters an object that is bigger than the wave itself, and in turn is bounced off in another direction (Coleman & Westcott, 2012). The two major types of reflection are called sky wave reflection and microwave reflection (Coleman & Westcott, 2012). Sky wave reflection occurs in frequencies below 1 GHZ that bounce off the surfaces of charged particles of the ionosphere (Coleman & Westcott, 2012). This is why you can be in Chicago, IL and still listen to radio stations in Los Angeles, CA (Coleman & Westcott, 2012). Microwave reflection happens in higher frequencies between 1 GHz and 300 GHz. These signals have smaller wavelengths and can bounce off smaller objects such as glass, walls, and metal doors or bigger objects such as buildings, and even the earth’s own surface (Coleman & Westcott, 2012). Microwave reflection is often the issue with signal degradation and performance problems when operating in Wi-Fi environments (Coleman & Westcott, 2012).

Scattering happens when the electromagnetic signal's wavelength is much larger than the object or pieces of the medium the signal reflected from causes the signal to be absorbed and then bounced or reflected into multiple directions (Coleman & Westcott, 2012). An example of this scattering can happen during sandstorms or when the atmosphere is filled with smog (Coleman & Westcott, 2012). Scattering can also occur when the RF signal encounters an uneven surface such as a chain link fence, tree foliage, or a rocky mountain, which causes the signal to scatter into multiple directions (Coleman & Westcott, 2012). This may be of concern if the wireless AP is placed in a secured space with fences or gates around it. This is a common physical security practice of units guarding communications suites or command posts.

Refraction and diffraction are the two RF propagation conditions that exist where the RF signal is actually bent (Coleman & Westcott, 2012). Not to be confused with each other, refraction occurs most commonly as a result of atmospheric conditions such as water vapor or changes in air temperature, causing the direction of the wave to change when the RF signal passes through a medium of a different density (Coleman & Westcott, 2012). Diffraction is the bending of the RF signal around the object or medium (Coleman & Westcott, 2012). An example of this condition happens when an object, such as a hill, partially blocks the origin of the signal and its intended destination (Coleman & Westcott, 2012).

Multipath occurs when two or more paths of a signal arrive at the destination antenna the same time (Coleman & Westcott, 2012). This is a result of the previously discussed RF propagation behaviors that cause signals to reflect and bend which takes them longer to arrive at their destination and is called the delay spread (Coleman & Westcott, 2012). Multipath causes the combined signal to attenuate, amplify, or become corrupted (Coleman & Westcott, 2012). Using directional antennas to reduce the number of reflections can mitigate the effects of multipath (Coleman & Westcott, 2012).

5. RF Spectrum

Burkhart (2004) believes that the Marine Corps and other DoD organizations' over dependence on the electromagnetic spectrum for communications has caused for the

frequent encounters in potential competition, interference, and coordination requirements for international and commercial frequencies. Burkhart (2004) states that, "Over the past decade the Government has ceded 247 MHz of bandwidth to industry—more than half in the desirable 3 GHz band." The military measures effectiveness of the spectrum in moving information from point to point as a matter of life and death (Burkhart, 2004).

The Federal Communications Commission (FCC) encyclopedia defines the RF spectrum as the radio frequency portion of the electromagnetic spectrum (www.fcc.gov, 2013). The FCC and the National Telecommunications and Information Administration (NTIA) regulate the RF spectrum. The FCC manages the spectrum for non-Federal agencies and the Federal agencies are managed by the NTIA (www.fcc.gov, 2013). Figure 3 depicts the Wi-Fi Radio spectrum of the electromagnetic spectrum.

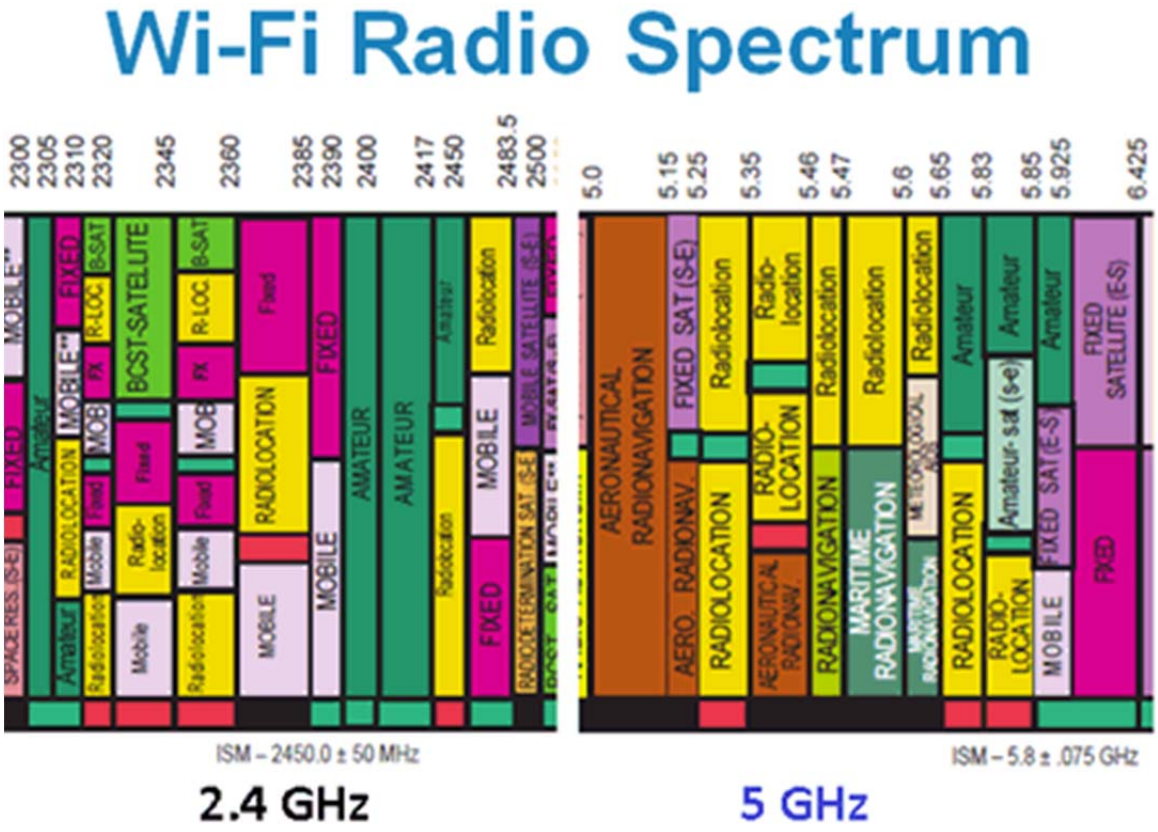

Figure 3. Wi-Fi Radio Spectrum and Services Chart
(From U.S. Department of Commerce, 2003)

C. STANDARDS ORGANIZATIONS

There are numerous standards organizations and regulatory bodies that govern and regulate communications and the usage of wireless technology (Coleman & Westcott, 2012). It is important to become familiar with these different organizations and the roles and responsibilities they have with wireless communications to help develop awareness and increased understanding of the technology, because it is a field that constantly changes.

In the United States, regulatory responsibility for setting the rules on the radio spectrum is divided between the Federal Communications Commission, which answers to Congress, and the International Telecommunication Union Radio Communication Sector (ITU-R), which answers to the executive branch of government (Burkhart, 2004). The ITU-R is a specialized United Nations agency that coordinates telecommunications matters among member countries. Use of the radio spectrum is largely coordinated through the ITU-R radio communications sector, which develops technical coordination criteria and standards for such use, and through various periodic conferences attended by member nations of the ITU-R (Burkhart, 2004).

The Institute of Electrical and Electronics Engineers (IEEE) has a collaboration of well-respected people in the computer industry, and creates the standards for compatibility and interoperability between networking systems all while adhering to the rules of its oversight organizations, such as the FCC (Coleman & Westcott, 2012). Then there are nonprofit industries such as the global Wi-Fi Alliance that market and raise consumer awareness to new wireless technologies as they are introduced (Coleman & Westcott, 2012). Another important organization is the International Organization for Standardization (ISO), a global, nongovernmental organization that partners and develops standards for business, government, and consumers' needs (Coleman & Westcott, 2012). Acquisitions and communications personnel working in the information technology field should stay abreast of the latest technology and news.

D. TYPES OF WIRELESS TECHNOLOGIES

This chapter is dedicated to a discussion of the different Wi-Fi technologies that are available in the commercial and military sectors today. Knowing the different technologies available will help with the understanding and ability to articulate the capabilities for the acquisitions and/or communications personnel responsible for acquiring, implementing, planning, and employing these devices. Below is a summarization of the current available wireless technologies.

1. EEE 802.11a

Brain, Wilson, and Johnson (n.d.), state, "IEEE 802.11a transmits at 5 GHz and can move up to 54 megabits of data per second." It uses orthogonal frequency-division multiplexing (OFDM), which is a coding technique that splits the radio signal into several sub signals before it reaches the receiver, a process that greatly reduces interference (Brain et al., n.d.).

2. IEEE 802.11b

IEEE 802.11b is probably one of the cheapest and slowest standards available (Brain et al., n.d.), and uses complementary code keying (CCK) modulation and transmits in the 2.4 GHz frequency band transferring up to 11 megabits of data per second (Brain et al., n.d.).

3. IEEE 802.11g

Like IEEE 802.11a, IEEE 802.11g use OFDM coding techniques but shares the 2.4 GHz frequency band of the radio spectrum like 802.11b (Brain et al., n.d.). Although IEEE 802.11g and IEEE 802.11b transmit in similar frequency bands, IEEE 802.11g is faster than IEEE 802.11b and can handle speeds up to 54 megabits per second (Brain et al., n.d.)

4. IEEE 802.11n

IEEE 802.11n has become one of the most exciting and widely available standards (Brain et. al., n.d.). It uses the APs and clients' antennas to transmit multiple

and simultaneous data streams (White Paper, n.d.). The resulting effect is both increased throughput and increased range (White Paper, n.d.). IEEE 802.11n can transmit up to 140 megabits per second (Brain et. al., n.d.) and 802.11n is backwards compatible with IEEE 802.11a,b, and g standards (Brain et. al., n.d.).

5. IEEE 802.11ac

A newer standard currently in draft form at the IEEE (but you may be able to find products for on the market), is IEEE 802.11ac (Brain et. al., n.d.). IEEE 802.11ac is backwards compatible with IEEE 802.11a, b, g, and n standards and transmits at either 2.4GHz or 5GHz frequency bands (Brain et. al., n.d.). IEEE 802.11ac is stated to be the fastest of the Wi-Fi standards with the ability to handle a maximum of 450 megabits per second on each of its multiple streams (Brain et. al., n.d.).

6. IEEE 802.16

IEEE 802.16, also referred to as the Worldwide Interoperability for Microwave Access (Wi-MAX), is a wireless technology based on a point-to-point broadband wireless access that uses microwaves to transfer data over distances over several kilometers (Jindal et al., 2004). Wi-MAX is based on the IEEE 802.16 wide area communications standards and has data rates that can reach up to 75Mb/s and has devices that works in the signals ranging anywhere from 2 GHz to 66 GHz (Mitchell, 2013).

7. Bluetooth

Dhawan (2007) defined Bluetooth as a wireless technology where all mobile devices are connected in range of one mobile device. It was created to be used in mobile devices like laptops, cell phones, and LANs, but can now be found in other devices such as cars, video games, headsets, and other commercial electronic devices. Bluetooth technology was invented by Ericsson in 1994 and worked using the 2.4 to 2.48 GHz radio frequency spectrums (Palmer, 2012).

8. Wave Relay

Wave Relay is an advanced mobile ad hoc networking (MANET) solution that goes beyond the standard "self-forming" and "self-healing" mesh network and was developed by Persistent Systems. Instead, Wave Relay quickly and continuously adapts to fluctuations in terrain and other difficult environmental conditions to maximize connectivity and communication performance (www.persistentsystems.com, n.d.). The Wave Relay proprietary routing algorithm allows users to incorporate vast numbers of meshed devices into the network in which the devices themselves form the communication infrastructure (www.persistentsystems.com, n.d.) Figure 4 is an illustration of a wave relay network architecture created by students at the Naval Postgraduate School.

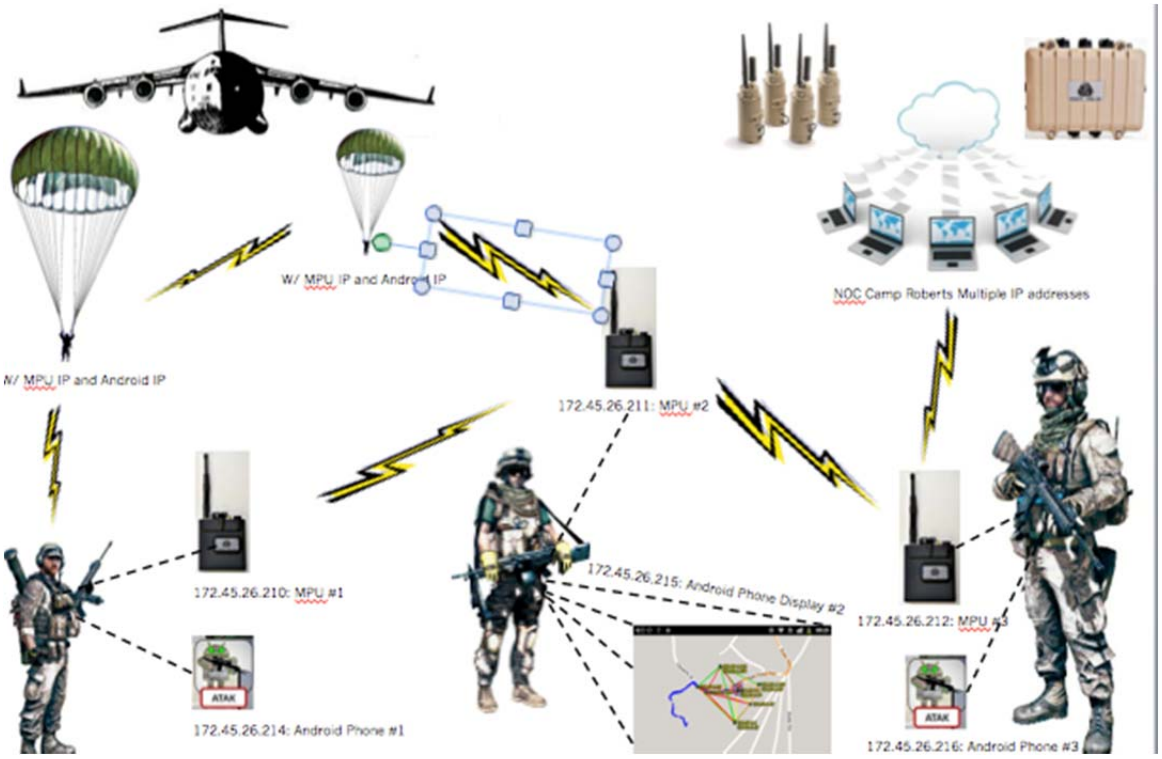

Figure 4. Wave Relay Architecture (After www.persistent.com, 2013)

E. WIRELESS COMMUNICATIONS

Dhawan (2007) discussed how increasing demand for mobile devices and the flexibility and mobility of the wireless technology have fueled the push for organizations to implement wireless technologies. In this chapter, the benefits and risks of adopting or implementing a wireless communications solution in an organization such as the Marine Corps will be discussed. The Marine Corps' vision of a wireless solution is one that provides a common, scalable, and interoperable solution from the company level up to the MAGTF level. This solution should not only save money and make logical sense, but it should also enhance the ability to Command and Control.

1. Benefits of Wireless Solutions

The answer to the question of the feasibility of wireless technology in a Marine Corps COC from a technological argument is *yes*. Wireless devices can be installed in a Marine Corps COC as easily as a home local area network. There are other issues that will be discussed later that prevents this technology from being implemented into the COC such as compatibility, costs, and regulations that dictate the implementation of this technology into existing systems, that will be covered later on in this chapter. This section will focus specifically on the applications such as data, voice, and video that have benefited with the expansion, availability, and technology improvements to the wireless networking infrastructure (Coleman & Westcott, 2012).

A benefit of wireless technology and communications is the increased mobility it offers. No longer is the user bound to a cable medium. A common misconception discussed by O'Sullivan (2001), is that *wireless* and *mobility* are synonymous. O'Sullivan (2001) states that they're different because *wireless* addresses media access sharing issues whereas *mobility* is about routing and addressing issues. Although it is possible to have mobility without wireless technologies, the always-connected network organization the Marine Corps and other DoD entities have adopted benefits substantially from wireless technologies (O'Sullivan, 2001).

Another benefit of wireless technology is the increase in speed with both installation and uninstallation of a network of many users (O'Sullivan, 2001). An

organization gains valuable time in establishing their networks and tearing them down because of the absence of wire needing to be ran during installation and recovered during uninstallation (O'Sullivan, 2001).

Another advantage of wireless technology is it allows for increased flexibility and scalability of an organizations' network (O'Sullivan, 2001). A wireless network can instantaneously be scaled to allow for a sudden increase in users as long as the users are in line of sight of the AP. Multiple APs allows for increased distances where non-collocated users can also connect to the wireless network.

2. The Risks of Wireless

Albert, Garstka, and Stein's (2009) *Network Centric Warfare* states that "Risk translates directly into increased costs and/or reduced value. Hence, the reduction of risk and its proper management are an inherent part of value creation. Network Security professionals such as John Fulp refer to risk in networking using a Risk Equation. The Risk Equation is written as "Risk = Threats x Vulnerabilities x Impact/ Security Controls" (J.D. Fulp, lecture, August 12, 2013).

So what are risks? Risks have the potential to disrupt or deny wireless communications. A lower risk value is more acceptable than a higher value. Threats are the identified or perceived issues that have been found to inflict harm to the intended operation of a wireless technology. The major cyber threats are security concerns. Vulnerabilities are the attributes of wirelesses design that results in intentional and/or unintentional problems (J. D. Fulp, lecture, August 12, 2013). An impact refers to the amount or type of damage that will be inflicted in correlation to a threat if it is unaddressed. When looking at impacts it is important to use the lens of the confidentiality, integrity, and availability (CIA) triad as it relates to costs, information assurance (IA), and mission-readiness (J. D. Fulp, lecture, August 12, 2013). The CIA triad will be discussed more in detail in the paragraph on security concerns and threats.

3. Security Concerns and Threats

Due to the expanded ability to deploy wireless technologies and applications into areas previously thought as inaccessible have created a myriad of security concerns as well. J.D. Fulp (2013) uses the term “CIA triad” to describe the three core information security objectives (lecture, August 12, 2013). Fulp states “Confidentiality is defined as the assurance that information is not disclosed to unauthorized individuals, processes, or devices. Integrity: guarding against improper information modification, and includes ensuring information authenticity. Availability: timely, reliable access to data and information services for authorized users” (lecture, August 12, 2013).

a. Types of Attacks

An attack is a threat that is carried out against a vulnerability that may exist in a wired or wireless network (Stallings et al., 2008). According to Coleman and Diener (2007), attacks are either intentional or unintentional. Intentional attacks are those that (as the name states) are done intentionally by a perpetrator with the intent to disrupt Wi-Fi communications through jammers, hacking and other malicious computer activity (Coleman & Diener, 2007). “This type of attack can both cause denial of service (DoS), and breaches that provide illicit access to the network” (Coleman & Diener, 2007). Unintentional attacks come from common devices that share the unlicensed spectrum with Wi-Fi, such as cordless phones and Bluetooth devices. Even devices not used for communication, such as microwave ovens; transmit RF in this spectrum, potentially disrupting Wi-Fi communications. “This type of RF interference can cause Wi-Fi users to experience degradation of throughput, increased latency, and loss of connectivity” (Coleman & Diener, 2007).

Rogue Access Points. Major oversights in most current wireless intrusion detection systems (WIDS) solutions are the inability to identify security threats at layer 1, the physical layer of the OSI model (Coleman & Diener, 2007). One major layer 1 security risk is undetectable rogue access points. Rogue access points are 802.11 devices that are connected by some malicious person to an 802.3 Ethernet port giving him a portal and access to attack from within your network infrastructure (Coleman & Diener,

2007). Examples of these rogue devices are the Bluetooth radios found inside some laptop computers, which allow them to plug into your router through the Ethernet port. A layer 2 WIDS or wireless Internet protection system (WIPS) are recommended solutions in order to detect and prevent the effects of these rogue devices (Coleman & Diener, 2007).

Denial of Service Attacks. According to Fulp, Denial of Service Attacks (DoS) is another threat to Wi-Fi security, in which the attacker attempts to disable your network by overworking your networks bandwidth, processor, and/or memory (lecture, August 12, 2013). These types of attacks are most common at layer 2 as well as at layer 1, and are considered to be serious threats toward mission critical tasks because it has the capability to compromise the availability of your systems and network (Coleman & Diener, 2007). An example of a DoS attack is the jamming effect by an electronic counter measure (ECM) device preventing the operation of radio and cell phone used to detonate improvised explosive devices (IED) in Iraq. These were layer 1 devices that intentionally or unintentionally denied service to any device operating within a specific spectrum by producing more power than the other devices using that spectrum. DoS attacks at the Layer 2 level, however, can be difficult to prevent but are easy to detect with WIDS devices and software (Coleman & Diener, 2007). The most common DoS attacks come from unintentional interference from devices such as microwaves and other devices operating on the same frequency as your wireless network.

Authentication Attacks. The request for comments (RFC) 2828 document states that authentication attacks occur when an attacker compromises the authentication process in order to gain access into the wired or wireless network (Shirey, 2000). RFC 2828 states that the authentication process consists of identification step, providing a approved user identification name, and then a verification step, providing a password to verify you are that user (Shirey, 2000). Most authentication attacks are against vulnerabilities in passwords. Today many organizations as well as the Marine Corps have adopted and implemented Information Assurance (IA) programs where the focus is training on areas such as password protection and password generation procedures and

practices in order to help prevent against dictionary attacks and other password hijacking techniques.

Evil Twin Access Points. Evil Twin Access Points refers to attacks in which Wi-Fi users are tricked into connecting to a pretentious wireless AP Phifer (2011). "Also known as AP Phishing, Wi-Fi Phishing, Hot spotter, or Honeypot AP, these attacks use phony APs with fake log-in pages to capture credentials and credit card numbers, launch man-in-the-middle attacks, or infect wireless hosts" (Phifer, 2011). There is WIDS software available that helps detect these types of attacks, for example Internet Browsers such as Microsoft Internet Explorer and Firefox have implemented security padlocks to indicate that a website is authentic and secure.

Man-in-the-Middle. RFC 2828 defines the Man-in-the-Middle attacks as when an attacker intercepts and modifies data that was communicated between two parties and then pretends to be one of the intended recipients or the sender (RFC 2828).

Eavesdropping. Eavesdropping is when wiretapping is done passively and secretly in order to intercept information from two communicating parties (RFC 2828).

4. Vulnerabilities and Limitations of Wireless Networks

Rappaport (2006) discussed some of the limitations and vulnerabilities in wireless networking compared with fixed wired networks (p. 443). A problem unique to wireless communications that Rappaport (2006) discussed was the hostile and random nature of the radio channel, and since users may request services from many different locations while traversing over wide areas, APs must be in place that can seamlessly handle this possible constant change of location while keeping the user connected (Rappaport, 2006, p. 444). Historically, and the argument is it still holds true today, the user requirements for wireless communications has exceeded the capacity of the available technology and resources such as routers and APs (p. 443). Because of the proliferation of wireless networks in homes and workplaces, people have become familiar with the technology, as a result demand along with high expectations of quality of service have increased to a point that may or may not be supplied by the provider.

S. Jindal et al., (2004) described vulnerabilities inherent with two wireless technologies, 802.11b and 802.11g, in that it uses the crowded 2.4 GHz spectrums. A 2.4 GHz spectrum is the spectrum also used for common devices such as microwave ovens, cell phones, cordless phones, and Bluetooth-enabled devices (Jindal et al., 2004). Similar devices on a network that share the 2.4 GHz spectrums have the potential to cause degradation in the performance of your wireless network (Jindal et al., 2004). Jindal et al. (2004) also discussed the issue of power consumption as a key vulnerability because 802.11b/g standard power consumption is fairly high compared to other standards, causing battery life and overheating to be of concern.

5. Impacts

Impacts of wireless technology for a military institution can be examined through several lenses such as cost, operation, information assurance, and loss of life or critical resources. Managing costs is critical considering today's financial climate, where budgets are decreasing and spending is being more scrutinized. Operations can be either positively or negatively impacted significantly by wireless technology, especially if a unit's wireless communications infrastructure is its single point of failure. Information assurance has been given a lot of attention as of late in the Marine Corps and DoD as a whole due to the increased availability and usage of wireless and similar technologies. If wireless technology can increase effectiveness and efficiencies of an organization's C2, then lives and other valuable resources can be positively affected.

6. Security Controls

When discussing risks such as the threats, issues, and problems associated with Wi-Fi technology as above, it is also appropriate to provide a possible solution and/or way to mitigate the threat. One such solution that mitigates the threat to information assurance is practicing good information awareness and providing information assurance training. One can read and/or PDF files of current and draft Federal government security policies, regulations, and publications on the National Institute of Standards and Technology's Security Division website www.csrc.nist.gov.

III. DISCUSSION OF THE CURRENT MARINE CORPS COC

A. BACKGROUND

In 2012, the Marine Corps Systems Command (MARCORSYSCOM) put out a document soliciting thesis research on the topic of providing acquisitions personnel with information that would help them better articulate the benefits of a wireless communications solution within a Marine Corps COC. The purpose of this chapter is to provide a summarization of different wired and wireless communications and networking equipment, mediums, standards, and regulations currently in place throughout the command echelons in the Marine Corps. This will provide the acquisitions and communications personnel with general background and understanding of the current capabilities, standards and regulations, and equipment, enabling them to better articulate and/or reference the subject of both wired and wireless communications that are currently employed throughout the Marine Corps. The chapter begins by covering the Marine Corps current guidance and standards on the operation of wireless network clients on a Marine Corps network. The second section of this chapter is dedicated to the current Marine Corps communications network and Combat Operations Center (COC) CapSet solution employed by different echelons of the Marine Air Ground Task Force (MAGTF).

B. USMC GUIDANCE ON WIRELESS NETWORKS AND DEVICES

In July 2007, the Marine Corps Command, Control, Communications, and Computers (C4) Information Assurance Division published the *Marine Corps Information Assurance Enterprise Directive (IAED): 014 Wireless Local Area Networks (WLANs) V2.0 Directive*. The document's purpose was to provide instructions governing DoD Information Assurance (IA) and outline the security configuration and implementation standards for WLANs in the Marine Corps Enterprise Network (MCEN) (Marine Corps IAED 014 WLANs v2.0, 2007). The Marine Corps IAED (2007) objectives were to ensure that the Marine Corps:

- Protect the confidentiality, availability, authentication, integrity, and non-repudiation of both wired and wireless IT assets, including information transmitted using commercial WLAN wireless devices, services and technologies
- Wireless IT assets do not adversely impact existing systems by causing electromagnetic interference (EMI) or other unintended electromagnetic consequences as determined by the FIPS 140–1, Security Requirements for Cryptographic Modules, 25 May ‘01
- Wireless technologies are afforded the safeguards required to protect USMC IT assets from the vulnerabilities associated with the use of commercial wireless local area networking technologies
- Personnel using USMC information systems receive wireless security training commensurate with their duties and responsibilities
- Wireless security-related technology research and development efforts are responsive to the requirements of the USMC
- Encourages interoperability between Department of the Navy (DON) enclaves and DoD agencies, as required

The Marine Corps IAED (2007) applies to all Marine Corps components, organizations, and personnel including systems directly connected to the Marine Corps Enterprise Network (MCEN) backbone and any other networks used to process both standalone and contractor-provided USMC data. The MCEN backbone is defined as “all garrison, tactical and Navy Marine Corps Intranet (NMCI) networks that operate in accordance with the Marine Corps IAED 014 WLANs v2.0 (2007) section 1.3.1.” The IAED (2007) also classifies the use of commercial wireless networking technologies into two zones as well as list those devices and systems that do not apply to the IAED are shown in Table 2.

Zone 1	Zone 2	Devices that Do Not Apply
All wireless networks using commercial wireless technologies, that connect to the MCEN backbone, and/or stores, processes, or displays USMC operational data, processes any information that is sensitive in nature or any other information that may be considered DoD SBU.	All wireless networks using commercial technologies, which do not fit into Zone 1, such as dedicated point-to-point RF connections secured by a FIPS 140 approved solution that operates at or above Layer 3 of the OSI model, or an infrastructure solution secured by the Harris Sec Net 54 Type 1 solution.	Receive only pagers, GPS receivers, hearing aids, pacemakers, Blue tooth devices (mice, keyboards, printers and other peripheral devices), Radio Frequency Identification Device (RFID) technology

Table 2. IAED Zones and devices that do not apply (After IAED, 2007).

According to the IAED (2007) cellular wireless technologies are allowed to connect to the MCEN as long as they are secured in accordance with current publications of the remote access service (RAS) policy and have the necessary data encryption technology approved by the DAA security solution. The IAED (2007) states that the "current policy does not support using a wireless client on any non-USMC approved wireless network to access a government/military network." An example of this would be using your wireless client or device to access the MCEN from a hotel or airport wireless network hotspot (IAED, 2007).

C. DOD GUIDANCE ON USE OF COMMERCIAL WLAN DEVICES

The purpose of DoDD (DoD Directive) 8100.2 (2007) is to "establish policy and assign responsibility for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG)." It is important for acquisitions personnel and communications planners to understand these references before purchasing and employing wireless technologies in their networks.

DoDD 8100.2 policy states that:

> 4.1. Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoD Directive 8500.01E and DoD Instruction 8500.02 and be certified and accredited in accordance with DoD Instruction 5200.40.

4.2. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).

4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

4.4. Pursuant to subparagraph 4.1.2, DAAs shall ensure that Wireless Personal Area Network (WPAN) capability is removed or physically disabled from a device unless FIPS PUB140–2-validated cryptographic modules are implemented (reference (g)). Exceptions may be granted on a case-by-case basis as determined by the DAA.

4.5. The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement.

4.6. Mobile code shall not be downloaded from non-DoD sources. Downloading of mobile code shall only be allowed from trusted DoD sources over assured channels.

4.7. PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.

4.8. Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data, in accordance with reference (e). The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency.

4.9. The DoD Components shall seek and follow spectrum supportability guidance from the Military Communications-Electronics Board (MCEB) prior to assuming any contractual obligations for the full-scale development, production, procurement, or deployment of spectrum

> dependent (i.e., wireless) devices or systems, in accordance with DoD Directive 4650.01.
>
> 4.10. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.

The use of commercial WLAN devices, systems, and technologies in the DoD GIG (U.S. Department of Defense, 2007) is discussed in the above memorandum from the Assistant Secretary of Defense, Network and Information Integration department. The policy provides supplemental guidance to DoDD 8100.2, with the goal of enhancing overall security and creating a roadmap for interoperability that embraces the IEEE standards for wireless or cellular technologies (U.S. Department of Defense, 2007). The policy states "WLAN devices, systems, and technologies must be acquired, configured, operated, and maintained to ensure joint interoperability, open standards, and open architectures per DoD Directive 8100.2 and DoD Instruction 8551.1 (U.S. Department of Defense, 2007). Any new acquisition of WLAN devices, systems, and technologies must comply with IEEE 802.11 body of standards (U.S. Department of Defense, 2007).

D. CURRENT USMC COC SOLUTIONS

Lawlor (2004) reported that in 2002, General Dynamics Decision Systems located in Scottsdale, Arizona, was awarded a five-year contract worth $13.4 million to develop the current Marine Corps COC CapSets. The Combat Operations Center (COC), originally known as the unit operations center (UOC) when it first came out, is designed to provide centralized Command and Control operational facilities to collect, process, and disseminate tactical data for the commander and staff of a Marine battalion/squadron. The COC CapSets was a commercial off-the-shelf (COTS) solution to fill a mobile C2 capability gap for the Marine Corps MAGTFs. The Marine Corps Components tock document for the COC provides the following technical data description:

> The COC is a High Mobility Multipurpose Wheeled Vehicle (HMMWV) trailer-based system that provides tactical commanders with a Common Operational Picture (COP) and integrated tactical data and communications assets needed to plan and conduct operations in an expeditionary combat environment. The system enables analytical and

intuitive decision-making with a modular and scalable equipment set consisting of a common module Operational Facility (OPFAC), C2 system, visual displays, and software.

Manufactured by General Dynamics Decisions Systems, the Marine Corps COC CapSets currently come in four variations: CapSet I, designed for the Marine Expeditionary Force (MEF) level echelons; CapSet II, designed for the Marine Subordinate Command (MSC) level echelons; CapSet III, designed for the regimental, Marine Wing Squadrons (MWSG), Marine Expeditionary Units (MEU) level echelons; and CapSet IV, designed for the Battalion, Marine Air Group (MAG), and Marine Wing Support Squadrons (MWSS) level echelon (Lawlor, 2004). All CapSets come with a standard basic package, which includes laptops and tables, tents, a mobile communications trailer, and a mobile generator. All CapSets are hardwired with Ethernet cables that connect the end user devices to a switch/router combo found in the communications trailer.

The differences between the CapSets are usually based on the equipment and tactical data systems (TDS) capability found in each CapSet based on the level of the echelon for which it is meant. Figures 5 and 6 depict COC CapSets versions III and IV, respectively.

Figure 5. COC CapSet III (From USMC, 2005)

Description and Function. The Combat Operations Center (COC), Tactical Command System, AN/TSQ-XXX (V) 3 is a set of Commercial-Off-The-Shelf (COTS) equipment configured as a Capability Set III (CapSet III) tailored to the Regiment/Group level and is designed to provide a self-contained Command and Control (CÇ) operational facility to collect, process, and disseminate tactical data for the Marine Air Ground Task Force (MAGTF) commander and staff. The illustrations depict a CapSet III AN/TSQ-XXX (V) 3 deployed for operation and stowed ready for movement. COC displacement relies on three (3) owning unit M1123 High Mobility Multipurpose Wheeled Vehicle (HMMWV)-A2s as the prime mover. Up to 24 owning unit provided external radios may be connected to the COC voice communication system. Antennas can be located up to 2 km away using supplied fiber optic cable. (USMC, 2005)

Figure 6. COC CapSet IV (From USMC, 2005)

Description and Function. The Combat Operations Center (COC), Tactical Command System, AN/TSQ-XXX (V) 4 is Commercial-Off-The-Shelf (COTS) equipment configured as a Capability Set IV (CapSet IV) tailored to the Battalion/Squadron level. It provides a self-contained Command and Control (CÇ) operational facility to collect, process, and disseminate tactical data for the CE, GCE, CSSE, and ACE commanders and their staff. The picture depicts a CapSet IV deployed for operation. CapSet IV COC displacement relies on two (2) owning unit M1123 High Mobility Multipurpose Wheeled Vehicle (HMMWV)-A2s as the prime movers. Up to 24 external radios may be connected using the two Digital Switching Units (DSU); antennas can be located up to 2 km away using fiber optic cable. (USMC, 2005)

E. USMC IT BUDGET ANALYSIS

The Department of Defense has been faced with a multitude of budget cuts across the board. *Marine Corps Times* staff writer Tilghman (2013) writes in a news briefing on 31 July 2013 that Secretary of Defense Chuck Hagel outlined the blunt choices that the DoD are facing under the current sequestration where all military services are forced to take a 10 percent cut across the board. Tilghman (2013) goes on to discuss that Hagel outlined the conclusions of the strategic review where he discussed what the trade-offs will have to be between the capacity and the capability of our military forces. The Office of Management and Budget's (OMB) document offers a proposed fiscal year 2014 budget for the DoD of $526.6 billion (Internet source: www.budget.gov). This is a $3.9 billion or a 0.7 percent decrease from the 2012 budget (Internet source: www.budget.gov). Ten percent cuts across the board and a 7 percent decrease in financial budgets pose a significant concern and constraint to the Marine Corps, which in 2012 made up only 8 percent of the budget. Figure 5 is snapshot of the summary of the Department of Navy's (DON) fiscal year 2014 budget overview taken from www.finance.hq.navy.mil website.

PB13 ($B)	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FYDP
Marine Corps	24.9	25.2	25.1	25.4	25.9	126.4
Navy	130.9	137.2	138.3	142.0	144.7	693.1
DON	**155.8**	**162.4**	**163.4**	**167.4**	**170.6**	**819.6**
PB14* ($B)						
Marine Corps	24.2	25.1	25.0	25.2	26.1	125.6
Navy	131.6	137.9	138.6	141.2	143.7	693.0
DON	**155.8**	**163.1**	**163.6**	**166.3**	**169.8**	**818.6**
Delta PB13 to PB14						
Marine Corps	-0.7	0.0	-0.1	-0.2	0.2	-0.8
Navy	0.7	0.7	0.3	-0.9	-1.0	-0.2
DON	**0.0**	**0.7**	**0.2**	**-1.1**	**-0.8**	**-1.0**

Figure 7. DON FY 2014 Budget Overview (Office of the Secretary of the Navy Financial Management and Comptroller, 2013)

Organizations such as the DON and USMC are reducing their IT infrastructure costs and cyber vulnerabilities by consolidating Enterprise IT contracts, data centers, and improving IT governance (Office of the Secretary of the Navy Financial Management and Comptroller, 2013). In the midst of the current and projected fiscal challenges along with a minute representation of the DoD's fiscal budget, the Marine Corps must be able to maintain both capacity and capability while continuing to modernize its IT capabilities. According to McFarland in the Marine Air Ground Task Force's fiscal year 2012 C2 Roadmap PowerPoint brief, the Marine Corps' goals are to reduce the structure of the Marine Corps, modernizing and reshaping it into a "middleweight force" able to meet the uncertainty and threats of a strained fiscal environment, budget cuts, and current challenges and challengers to our nation's security. As a result, critical decisions have to be made now and in the future regarding the procurement of new IT systems as well what to do with our legacy IT systems with the availability of what financial resources can buy. Figure 6 provides a snapshot taken from the DON's 2014 budget highlights Figure 5, which shows fiscal years 2012, 2013, and 2014 appropriations summary.

(In Millions of Dollars)	FY 2012	2013 PB Req	2013 Full Yr CR	2013 P.L. 113-6	FY 2014
Military Personnel, Navy	26,410	27,091	26,967	26,867	27,824
Military Personnel, Marine Corps	13,610	12,481	13,719	12,515	12,905
Reserve Personnel, Navy	1,909	1,899	1,947	1,872	1,892
Reserve Personnel, Marine Corps	640	665	649	657	677
Health Accrual, Navy	1,806	1,184	1,397	1,397	1,198
Health Accrual, Marine Corps	1,126	673	810	810	684
Health Accrual, Navy Reserve	236	142	169	169	135
Health Accrual, Marine Corps Reserve	135	81	98	98	81
Operation and Maintenance, Navy	39,179	41,607	38,354	41,548	39,945
Operation and Maintenance, Marine Corps	5,664	5,983	5,577	6,024	6,255
Operation and Maintenance, Navy Reserve	1,300	1,247	1,313	1,255	1,198
Operation and Maintenance, Marine Corps Reserve	271	272	273	277	263
Environmental Restoration, Navy	-	311	311	310	316
Aircraft Procurement, Navy	17,632	17,129	17,705	17,359	17,928
Weapons Procurement, Navy	3,202	3,118	3,210	3,033	3,122
Shipbuilding and Conversion, Navy	15,138	13,580	15,010	15,564	14,078
Ship Maintenance, Operations, and Sustainment Fund	-	-	-	2,379	-
Other Procurement, Navy	5,992	6,169	5,990	5,947	6,310
Procurement, Marine Corps	1,423	1,623	1,431	1,410	1,344
Procurement of Ammunition, Navy & Marine Corps	627	760	602	659	589
Research, Development, Test, & Evaluation, Navy	17,648	16,883	17,848	16,941	15,975
National Defense Sealift Fund	1,472	608	1,107	697	731
Military Construction, Navy & Marine Corps	2,119	1,702	2,101	1,547	1,700
Military Construction, Naval Reserve	26	50	26	49	33
Family Housing Construction, Navy & Marine Corps	115	102	102	102	73
Family Housing Operations, Navy & Marine Corps	375	378	370	378	390
Base Realignment & Closure	346	165	130	194	145
SUBTOTAL	**158,402**	**155,902**	**157,219**	**160,060**	**155,790**
Overseas Contingency Operations	14,899	14,230	14,230	14,012	-
Other Supplemental	1,409	-	-	-	-
TOTAL	**174,710**	**170,132**	**171,449**	**174,072**	**155,790**
BY SERVICE					
Navy	**143,182**	**139,344**	**139,883**		**131,615**
Marine Corps	**31,529**	**30,788**	**31,566**		**24,175**

Figure 8. DON 2014 Appropriations Summary (2013).

1. Current Marine Corps IT Procurement and R&D Programs

The next section talks about some of the Marine Corps' current research and development programs and acquisitions in IT.

a. Marine Corps Command and Control Modernization:

The Department of the Navy's FY 2014 Budget Highlights (2013) notes that in order to improve the command and control capability for the MAGTF, the Marine Corps is seeking to use fiscal year 2014 budget funds for the procurement and research and development of three Command and Control systems (NOTM, JBC-P, and CAC2S). The U.S. Department of the Navy's Contract (2012) reads that in 2013 the Marine Corps awarded *iGov Technologies*, Inc., in Reston, VA, a "$64,637,423 firm-fixed-price contract to modernize the existing hardware within the Marine Corps' Combat Operations Center (COC)." The U.S. DON Contract (2012) also discusses that this effort will update and modernize the COC to a single baseline while reducing size weight and power requirements, replacing routers and servers, etc. The U.S. DON Contract (2012) reads that this contract contains options, which if exercised, would bring the total contract value to $96,907,500 and that the Marine Corps System Command located in Quantico, VA, is the contracting activity (M67854–12-C-2429).

b. Marine Corps Radio and Switching Modernization:

In fiscal year 2014, the Marine Corps is looking to continue to procure tactical radio systems with the capability to support operational voice and data communications and other C2 requirements for static or mobile Marine units (Office of the Secretary of the Navy Financial Management and Comptroller, 2013). The 2014 budget also "allow the Marine Corps to continue to upgrade vehicular multi-channel radio systems with hardware and software that will increase bandwidth, reliability, and security for tactical command and control users" (Office of the Secretary of the Navy Financial Management and 2013). Furthermore, the Marine Corps will continue its procurement of Maintainer Training Systems for the Data Distribution System Modular (DDS-M), which provides LAN/WAN capabilities and makes up the MAGTF's data

communication backbone (Office of the Secretary of the Navy Financial Management and Comptroller , 2013).

IV. ECONOMIC ANALYSIS OF USMC EXISTING WIRED COC VS. WIRELESS

A. SWOT ANALYSIS WIRELESS VS WIRED COC

1. Wired COC

This section will analyze the Marine Corps CapSet model's strengths, weakness, opportunities, and threats. The analysis is based on the wired architecture of these COC systems.

a. Strengths

The strength of the current COC is all of its equipment is hard-wired and readily compatible with everything within the COC CapSets. The desks and tables of all the CapSets are all pre-wired with CAT-5 cable. This eliminates the messy runs of CAT-5 cable from the communication trailer's switches to the users' laptops, computers, and other network devices. COC users' devices are hard-wired, which also offers them the benefit of a reliable connection to the network and a network where services, as well as the devices, can easily be deployed, administered, monitored, and controlled by the managers of that network in any environment.

Another strength of the wired connection in the CapSets is its ability to transfer, download, and upload huge files and data across the network. Files such as Power Points and PDFs have the potential to be very large which can be problematic for some standards of wireless 802.11 technologies.

An additional strength of the COC's wired connection is the argument that hardwired technologies physically more secure than wireless. The idea rests behind the belief of current best security practices of most COC's, such as access restriction to spaces and physical barriers, an adversary wishing to commit certain denial of service (i.e., jamming), modification, and eavesdropping attacks on a network, ability would be physically hampered.

b. Weakness

A weakness of the current COC is the lack of (or limitations on) mobility because of its wired architecture. Although being wired has its strengths and benefits, it hampers the users' as well as the network administrators' and installers' flexibility to move and/or locate devices within or away from the COC without the installation of additional wiring outside of the COC CapSets pre-wired architecture. Figure 5 is an example of the clutter that can result from a wired installation in the current COC CapSets.

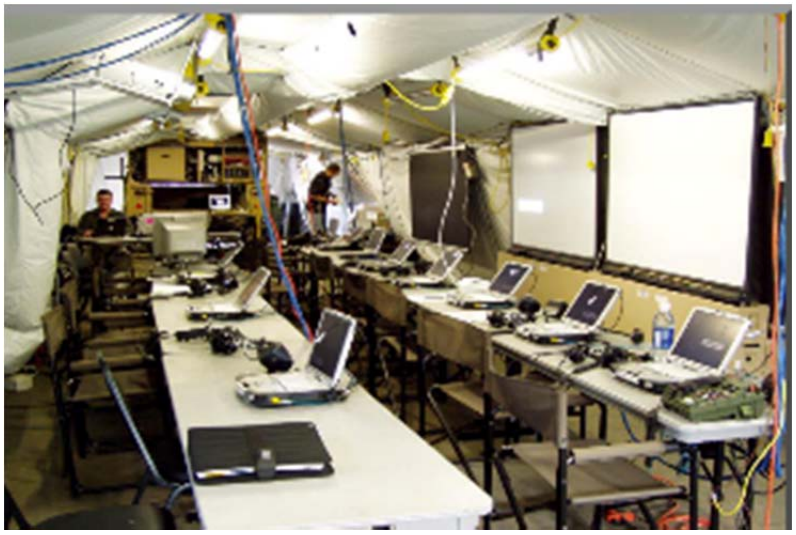

Figure 9. Wired CapSet (www.docstoc.com, n.d.)

"Moore's law" describes the principle dynamic of innovation in the semiconductor fabrication market (Albert, 2000). The idea is that the performance of computer technology can be expected to double approximately every 18 months (Albert, 2000). The current computer technology in the COC at the time of this writing is nearly ten years old. Following Moore's law, that means the current technology of the COC CapSets are quite outdated. Although firmware updates can extend the life of the software of a system, the system is still limited by its hardware, memory and processing

speed. The outdated nature of these systems can also create reliability problems as well as compatibility issues with newer equipment and newer technologies.

Another weakness of the wired architecture of the COC is the bulkiness of the entire system and accountability of thousands of pieces associated with the system. The setting up, tearing down, and logistics of getting the current COC CapSets can be problematic for owners of these systems, as well as the maintenance and accountability of the parts. Although the CapSets are mobile, coming with two trailers, one for the generator, and the other for the communications suite, there are probably twenty to thirty additional separate containers that house the parts for rest of the COC.

c. Opportunities

Although outdated, there are still opportunities available using the current technology and equipment of the wired COC infrastructure. One is a reduction of future spending on IT equipment and technology. With the introduction of cloud computing, the need for newer computer equipment such as hard drives, memory, processing power, etc., is lessened because the cloud can handle all of those responsibilities remotely. A user may not be able to or even have to physically move his device in the current COC setup, because all of the data has the potential to be accessed from the cloud infrastructure. The benefit of the cloud has the potential to extend the life of current COC systems where money for IT programs can be redirected elsewhere. Higher data throughputs, reliability, and the security of a wired connection in the COC are always giving many communications planners the opportunity to expand a communications infrastructure out to the users and still maintain control of both the devices and services on that network.

d. Threats

One threat that exists is the lack of program support for the current COC CapSet systems due to dwindling DOD budgets and funding that would be needed to sustain maintenance and upgrades to legacy systems in the COC CapSets. There is also the potential threat that the legacy systems in the COCs will be too outdated, making them incompatible with newer advantageous IT technology that is currently available or projected in the future. In Albert's (2000) *Network Centric Warfare* he states that the

"increasing availability and affordability of information, information technologies, and information Age weapons increases the potential for creating formidable foes from impotent adversaries" (p. 19). This can cause for a deterioration of any information dominance or advantages previously afforded by current technology and legacy systems in the CapSets, creating a disadvantage against current or potential adversaries who adopt these newer IT technologies (Albert, 2000).

2. Wireless

a. Strengths

Some strengths of adopting a wireless connection are the potential for an increase in flexibility, mobility, and scalability in a communications network. Incorporating a wireless solution allows the communications planner to grow and expand on the network architecture more easily and quickly because of the absence of additional physical installation that goes with a wired connection. It also allows for a quicker installation and is conducive to any sudden infrastructure modifications, device location changes, and increase in users. A wireless network's rapid ability to deploy expected or unexpected services reduces friction and decreases the use of messy wire runs and any installation difficulties or complexities associated with physically installing wires to the device and user. There is also the potential to extend networking capabilities outside the range of the COC to other authorized users within reach of the AP.

b. Weakness

Security has long been a concern and a weakness of wireless communications. The belief is that an unauthorized user can easily gain access or disrupt communications inside a network if he is able to get close enough to the AP. WLANs are a collection of wireless devices that are capable of maintaining connectivity with one another while transferring data without disruption (Ravichandiran & Vaithiyanathan, 2009). Ravichandiran and Vaithiyanathan (2009) discuss two fundamental configurations for wireless networks, peer-to-peer (P2P) and peer-to-multipoint (P2Mp). One of the issues with P2P configurations is that the two communicating endpoints must be close enough to mitigate the effects of RF interference or signal loss in order to communicate

effectively and with increased reliability (Ravichandiran & Vaithiyanathan, 2009). In P2Mp one centralized administrator, serving as the hub, associates with multiple nodes consisting of multiple wireless devices (Ravichandiran & Vaithiyanathan, 2009). An issue with P2Mp configuration is that connections are dependent upon the distance between the wireless devices, creating a region where the devices must stay within in order to prevent disruption of communication (Ravichandiran & Vaithiyanathan, 2009). Although these Wi-Fi networks can be quite inexpensive to install, the fact that the device's technology is dependent on line of sight (LOS) creates vulnerability (Ravichandiran & Vaithiyanathan, 2009). The problem comes when obstacles are placed in the way of these devices obstructing clear LOS and/or the proliferation of many wireless devices in a WLAN creating competition for resources such as throughput (Ravichandiran & Vaithiyanathan, 2009).

Another weakness that wireless technology has is that it is very vulnerable to intentional and unintentional. The RF propagation effects discussed in Chapter II can sometimes (and most times are) out of the control of the communications planner and installer. Common appliances found inside or near COC's such as a microwave, or metal concertina wires outside the COC, can cause distortion or interruption of the RF signals of a wireless network.

Range and data transfer speeds of a WLAN has the potential to be a weakness depending on what type of usage requirements a unit may have. Some units the size of a battalion may have large demands for streaming video and/or exchanging files that can bottleneck a wireless network, or its needs may not be satisfied by a wireless network. Although technology has improved substantially in wireless communication, it is still much slower and less reliable than wired.

With decreasing budgets, the future affordability of implementing a wireless solution may also be a weakness for some organizations. The ability to purchase a reliable, secure, commercial off-the-shelf COTS solution that meets all DoD specifications and requirements may come at a price that is unrealistically unattainable for an organization such as the Marine Corps. Research and development of a suitable

wireless solution may also be unachievable due to current and possibly future budget constraints.

c. Opportunities

A lot of attention has been given to the financial feasibility of acquiring or adopting newer information technology systems or programs, but wireless has the potential to save money for a DoD organization. An argument can be made for the ability to use personal devices such as a wireless laptop or smart phone on an enterprise network such as the MCEN. Organizations such as the Naval Postgraduate School have already installed and are currently operating networks that allow users to connect personal wireless capable devices securely to the NPS network infrastructure. This may not be a reliable solution for a highly sensitive classified network, but it is quite suitable for unclassified networks, especially in garrison environments on base. Adopting this strategy would force potential changes to current regulations and specifications that enforce security standards in the DoD, but it can be done.

There is also the opportunity to cut costs associated with the installation and maintenance with a wired connection. Wired connections have the potential to deteriorate over time or be cut due to unforeseen circumstances associated with operating in dynamic environments where hot temperatures and heavy trafficked areas are common. Using wireless connections can be a viewed as a sort of automation to the installation process in that less labor is needed to operate, install, and maintain wireless devices, resulting in lower expenses. Using wireless has the potential to decrease or eliminate costs for manpower, training, and maintenance. It also eliminates the need for a lot of heavy equipment that is currently part of the COC CapSets which can have anywhere from twenty to thirty additional containers that need to be accounted for, maintained, and moved from place to place. Cargo space and its weight costs money when it comes to transporting equipment and by decreasing the bulky equipment needed to operate and install a wired infrastructure, a reduction in cost may ensue. Wireless technologies can eliminate the need for a lot of the bulky equipment currently being deployed in the COC CapSet models.

d. Threats

One threat to using wireless technologies is its security, which potentially gives a determined adversary the ability to remotely disrupt services due to the advancements in wireless technologies and the readily available products that an attacker can acquire and use against a wireless infrastructure. Wireless attack tool kits such as the "Raspberry – PI" (shown in Figure 10), and instructions to use them are readily available to anyone who desires them. Although steps can be taking to safeguard against these type of devices within the immediate area, which are now being addressed with current information-awareness initiatives, disgruntled employees as well as an enemy can still use a tool such as the Raspberry – PI to perform attacks against a network from outside the controlled area or even inside the controlled area when considering an insider attack.

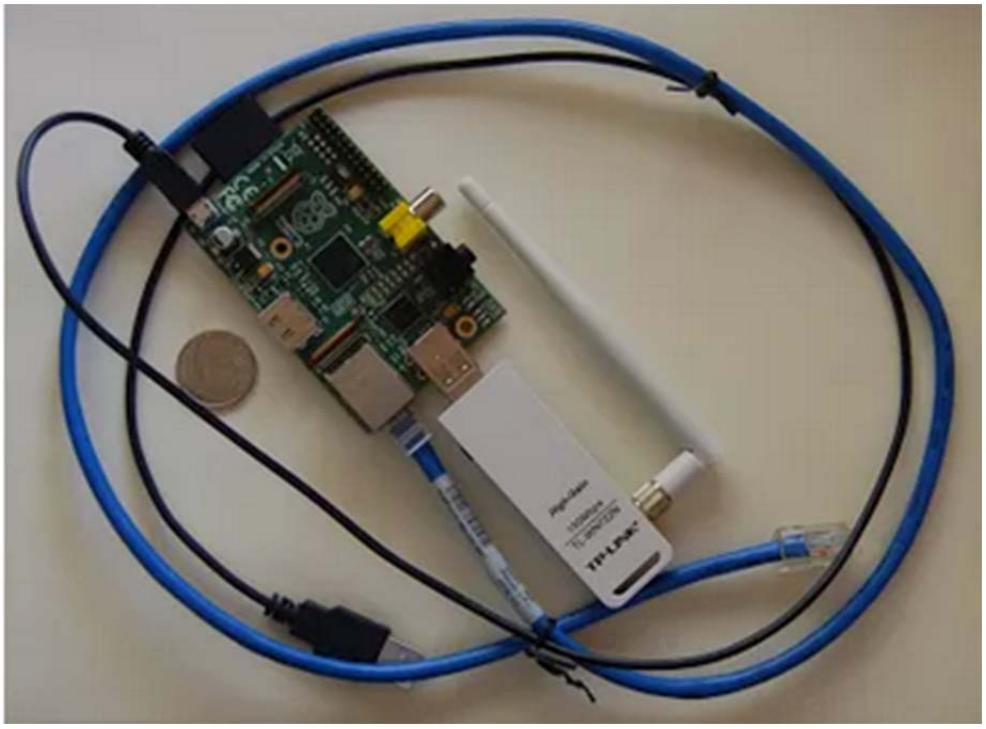

Figure 10. (From www.howtodocomputing.blogspot.com, n.d.)

Wireless –PI is "a collection of pre-configured or automatically-configured tools that automate and ease the process of creating robust Man-in-the-middle attacks. The toolkit allows you to easily select between several attack modes and is specifically designed to be easily

> extendable with custom payloads, tools, and attacks. The cornerstone of this project is the ability to inject Browser Exploitation Framework Hooks into a web browser without any warnings, alarms, or alerts to the user. We accomplish this objective mainly through wireless attacks, but also have a limpet mine mode with a few other tricks (www.howtodocomputing.blogspot.com, 2013).

B. COMPARISON OF WI-FI AND WIRED

Chiu, Y., Logman, Chiu, M., and Sunkara, (2005) discuss how wired and wireless technologies have continued to mature and innovate at an unbelievable rate (p. 3). Old technologies such as wire tend to be resilient, reliable, and robust even under harsh conditions and elements as well as offer high transfer speeds and data throughput (p. 3). Some 802.3 wire mediums such as CAT 5 may degrade and lose effectiveness over time and distance, but there are still faster and capable cables, such as fiber-optics, that can be employed over great distances and provide high rates of data throughput. Figure 11 shows characteristics of some current wired technologies.

Newer technologies such as wireless 802.11ac are starting to offer more speeds that are nearly comparable to wired connections while expanding on its ability to provide flexible configurations and other communications services (p. 3). Devices that work with wireless technologies have also decreased in size and weight along with increasing battery life to power the processers in these mobile devices.

The current Marine Corps CapSets models were contracted in the early 2000s. The communication suites supported currently in the COC are all wire-based, CAT 5, fiber, twisted pair, etc. In 2009 General Dynamics was awarded a $54 million dollar contract to replace the aging systems (*Defense Industry Daily Staff,* 2009). Below is a comparison of the highlights of advantages and disadvantages for the COC and wireless technologies in order to give the acquisitions and/or communications planner a quick guide to the strengths and weaknesses between the two options.

1. COC

a. Advantages

- Cost has already been spent to acquire, train, implement system into fleet
- Interoperability with other Marine Cops communications devices and radio systems
- Reliable and secure connections to the secure and non-secure LAN infrastructure

b. Disadvantages

- Outdated technologies
- Big and bulky equipment (communications trailer house switch and routers)
- Limited flexibility due to internal wiring of tables and other components in the COC.
- External wiring to expand network can become cluttered and confusing
- Numerous parts and SL-3 components can be a challenge to account for and maintain.

Existing Technologies	
Twisted-pair	Medium – copper wire Operates at 300 to 3,00 Hz Offers 56 bps with range 9 to 15 miles Support data, voice, slow scan TV
ISDN	Offers 64 kbps
ADSL (copper wire)	Offers 1.5 Mbps to 6.3 Mbps downstream, depending on wire gauge, protocol, and distance Support data, voice and video
ADSL (copper wire + satellite)	Offers 1.5 Mbps downstream, 128 kbps upstream Support data, voice and video
Cable	Medium – coaxial cable Operates at 5 to 350 MHz Offers 10 Mbps downstream, 1.5 Mbps to 10 Mbps upstream Support data, voice and video
Fiber-optics	Medium – fiber glass Operates using laser waves Offers from 10 Mbps to 10s Gbps Support data, voice and video, usually used in backbone network, now increasing used at access network
Upcoming Technologies	
Power Line	Medium – electricity power line Offers up to 15 Mbps data transfer rate Latest standard released in 2002z Field test in 2002 (Homeplug, 2002)

Figure 11. Wired Technology Characteristics (From Chiu et al., 2005)

2. Wireless

a. Advantages

- Technology promotes flexibility and mobility
- Data speeds and throughput are more than efficient to support current Marine Corps bandwidth transmission mediums and pipes
- Depending on budget limitations, option to purchase a wireless solution could save Marine Corps money and increase capability over current COC solution (section C in this thesis analyzes possible savings between the two technologies)
- Technology allows for faster expandability of a network
- Easier and neater installation

- Newer technology

b. Disadvantages

- Security issues with the technology
- Vulnerable to interference and other propagation effects discussed in Chapter II
- Not suitable for secure communications
- Has to be acquisitioned during a time of budgets constraints
- Limitations in bandwidth and throughput of current transmission systems do not support full capabilities of wireless technology.

C. COST ANALYSIS WIRELESS VS WIRED COC

Due to the potential sensitivity and proprietary nature of the data, some of the inputs/costs in this analysis will be done using fictional numbers in equipment, manpower, and costs to represent inputs/costs in order to keep the information in this document unclassified. The inputs/costs for wired technology for the COC and wireless technology solutions are based on estimates of unclassified historical and current comparative commercial market data as well as guesstimates of inputs/costs. A discussion of the data is provided to create a template that may allow for future researchers to easily re-create with sensitive pertinent data and calculations in their analyses. This data is intended only to give the acquisitions and/or communications planner and other invested decision-makers a close replica of what is needed to improve their understanding of the possible differences between wired and wireless communications.

1. Manpower Cost Savings

This data was created with the assumption that one enlisted Marine with the base pay grade of E-3 is the primary operator and installer of wire and associated equipment in a COC CapSet model. Table 6 shows the calculations for current and wireless manpower.

a. Current Manpower

- 10 x E-3 wireman make up an fictional BN
- 30 x E-3 wireman make up an fictional RGT
- 90 x E-3 wireman make up an fictional DIV
- 270 x E3 wireman make up an fictional MEF

b. Wireless Manpower (half of current manpower)

- 5 x E-3 wireman make up an fictional BN
- 15 x E-3 wireman make up an fictional RGT
- 45 x E-3 wireman make up an fictional DIV
- 135 x E3 wireman make up an fictional MEF
-

Current Manpower			
	Costs	**Month**	**Year**
	1 E3	$3,500.00	$42,000.00
BN	10 E3	$35,000.00	$420,000.00
RGT	30 E3	$105,000.00	$315,000.00
DIV	90 E3	$315,000.00	$3,780,000.00
MEF	270 E3	$630,000.00	**$7,560,000.00**
Wireless Manpower			
	Costs	**Month**	**Year**
	1 E3	$3,500.00	$42,000.00
BN	5 E3	$17,500.00	$210,000.00
RGT	15 E3	$52,500.00	$630,000.00
DIV	45 E3	$105,000.00	$1,260,000.00
MEF	135 E3	$472,500.00	**$5,670,000.00**

Table 3. Current Manpower and Wireless Manpower costs

2. Maintenance Cost Savings

This data was created based on 10 percent estimate of the contract cost of the initial investment of the COC CapSet contract of $650 million (*Defense Industry Daily Staff*, 2009).

a. Current Maintenance

- 1 x COC make up total systems in an fictional BN
- 3 x COC make up total systems in an fictional RGT
- 9 x COC make up total systems in an fictional DIV
- 27 x COC make up total systems in an fictional MEF

b. Projected Maintenance

- Costs are half of current costs

Current Maintenance			
	Costs	**Month**	**Year**
BN	1 COC	$1,000.00	$12,000.00
RGT	3 COC	$30,000.00	$90,000.00
DIV	9 COC	$9,000.00	$108,000.00
MEF	27 COC	$27,000.00	**$324,000.00**
Wireless Maintenance			
	Costs	**Month**	**Year**
BN	1 COC	$500.00	$6,000.00
RGT	3 COC	$15,000.00	$45,000.00
DIV	9 COC	$4,500.00	$54,000.00
MEF	27 COC	$13,500.00	**$162,000.00**

Table 4. Current Maintenance and Wireless Maintenance Costs

3. Transportation Cost Savings

This data was created based on a guesstimate of the weight, space, and cost of transporting one full 500 cubic feet of wired equipment per individual COC CapSet for one deployment. One iteration of a deployment counts as one deployment and one redeployment. The assumption has been made that a battalion deploys 1 time a year; a regiment deploys 2 battalions a year; a division deploys 4 battalions a year; and a MEF deploys 12 BN a year.

a. Current Transportation

- 1 x depl make up a fictional BN

- 2 x depl make up a fictional RGT
- 4 x depl make up a fictional DIV
- 12 x depl make up a fictional MEF

b. Projected Transportation

- Costs are half of current costs

Current Transportation			
	Costs	**Month**	**Year**
	1 move	$5,000.00	$110,000.00
BN	1 depl	$10,000.00	$220,000.00
RGT	2 depl	$10,000.00	$220,000.00
DIV	4 depl	$20,000.00	$440,000.00
MEF	12 depl	$30,000.00	**$660,000.00**
Projected Transportation			
	Costs	**Month**	**Year**
	1 move	$2,500.00	$55,000.00
BN	1 depl	$5,000.00	$110,000.00
RGT	2 depl	$5,000.00	$110,000.00
DIV	4 depl	$10,000.00	$220,000.00
MEF	6 depl	$15,000.00	**$330,000.00**

Table 5. Current Transportation and Wireless Transportation Costs

4. Miscellaneous Operating Expenses

This data was created based on guesstimate of expenses involved in the installation and operation of wired equipment in a COC CapSet. One example of an expense considered in the inputs is cost for spools of CAT 5 cable. Ten percent of the estimate of the $54 million modification contract awarded to General Dynamics for modification of the existing COC CapSets was broken down yearly and calculated into the expenses cost (*Defense Industry Daily Staff,* 2009).

a. Current Miscellaneous

- Estimation of $2,000 misc. expenses X number of COCs in MEF

b. Projected Miscellaneous

- Estimation of $2,000 misc. expenses X number of COCs in MEF
- 10% of cost used for modification investment ($54M) yearly

Current Miscellaneous		
Costs		**Year**
other expenses	$2000 x #depl(MEF)	$24,000.00
	Total Year	**$24,000.00**
Wireless Miscellaneous		
Costs		**Year**
mod (10% contract)		$5,400,000.00
other expenses MEF	$1000 x #depl(MEF)	$12,000.00
	Total Year	**$5,412,000.00**

Table 6. Current Miscellaneous and Wireless Miscellaneous Costs

5. Total Cost Savings

Total cost savings are calculated by taking the total differences between current (wired) and projected (wireless) for manpower, transportation, maintenance, and cost. These costs are added together to create the total cost savings for the year shown in Table 7.

Current Manpower	Wireless Manpower	Difference
$7,560,000.00	$5,670,000.00	$(1,890,000.00)
Current Maintenance	Wireless Maintenance	Difference
$324,000.00	$162,000.00	$(162,000.00)
Current Transportation	Wireless Transportation	Difference
$660,000.00	$330,000.00	$(330,000.00)
		$(2,382,000.00)
Current Miscellaneous	Wireless Miscellaneous	Difference
$24,000.00	$5,412,000.00	$5,388,000.00

Table 7. Total Cost Savings

6. Payback Period

The payback period answers how long it will take to recoup money in savings from the technology (Anthens, 2003). Some of these savings should go on forever, but an argument can be made that those cost savings just transfer to other priorities in the Marine Corps. The data in Table 7 was used to calculate the data in Table 8. Table 8 shows a comparison of payback periods for wired and wireless communications. The best option is determined by the least amount of time needed to break even or exceed the initial investment (Anthens, 2003).

	Payback Period	
	Wired	**Wireless**
Initial Investment	$650,000,000.00	$54,000,000.00
Year	Savings	
5	$26,940,000.00	$11,910,000.00
10	$53,880,000.00	$23,820,000.00
20	$107,760,000.00	$47,640,000.00
23		$54,786,000.00
121	$651,948,000.00	
Total	$651,948,000.00	$54,786,000.00
Payback Period	**121 years**	**23**

Table 8. Comparison of Wired and Wireless Payback Periods

D. REAL OPTIONS

1. Keeping Current COC CapSets

a. Strengths

- In the short run, less expensive than acquiring a new solution
- Still reliable, secure
- Marines are well trained with the system

b. Weaknesses

- Outdated technologies
- Bulky, beat-up equipment that needs to be refreshed

- May become incompatible with newer technologies that could potentially give the Marine Corps an information dominance disadvantage

2. Acquisition of a Wireless Solution

a. Strengths

- Could be expensive in the short run
- Addresses Marine Corps need of increasing mobility and flexibility
- Ability to deploy, install, and expand networks faster

b. Weaknesses

- Security and vulnerability of these systems to both outside and inside threats are increased
- Still costs money to acquire and maintain

3. Combining Both Wired and Wireless Solutions

Wired and wireless technologies can coexist and support each other. An option of acquisitioning a mixed wired and wireless solution while maintaining compatibility with current Marine Corps COC CapSet suites systems and capabilities could be a viable solution.

a. Strengths

- Less expensive than a new robust wireless-only acquisition
- Adds all advantages of wireless solution while using current COC capabilities to cover some of the weaknesses of wireless

b. Weaknesses

- Newer technologies may be incompatible with outdated COC legacy systems
- Still costs money to acquire and maintain

4. Other Possible Solutions

a. Using the Cloud

Hurwitz, Kaufman, Halper, and Kirsch (2012) describe cloud computing as a "method of providing a set of shared computing resources that includes applications, computing, storage, networking, development, and deployment platforms as well as business processes." Cloud computing is a technology that can create opportunities and advantages for the Marine Corps. The DOD has taken note of the capabilities of cloud computing and the advantages and benefits that can be gained from implementing this technology into their wired COC infrastructure (Wald, 2010).

The cloud offers advantages of elasticity and scalability of networks that can be designed to scale upwards and downwards on demand (Hurwitz et al., 2012). Another capability the cloud offers is that it is always available and accessible (Hurwitz et al., 2012). This offers an organization like the Marine Corps the ability for a unit to deploy or work from garrison to the battlefield seamlessly. Marine Corps units can easily access their data through a web based application from anywhere 24/7, without the need of an external removable storage device or deploying a users' garrison workstation with them, possibly eliminating the need for establishing an elaborate communications IT infrastructure or COC. The cloud may not serve as a definite alternative to adopting a wireless solution because the benefits of the cloud can be obtained using either wired or wireless connections, but it may serve as support to the reasoning in abandoning the heavy server, router, and wires that are currently used to connect devices to the network.

V. SUMMARY

With the evolution and introductions of the smart phone, tablet computers and other mobile connected devices in addition to the previous generation of desktop computers and VOIP phones, there has been an increase in demand for wireless mobile communications. Ravichandiran and Vaithiyanathan (2009) talk about factors such as the ones mentioned, that are driving the IEEE 802.11 wireless popularity in industry as well as the DoD. Once the footprint of devices grows so does the equipment needed to support those devices and possibly the personnel. Devices are now getting smaller and smaller and the demand for them to be wirelessly connected to the network has caught on throughout all sectors of industry. Ravichandiran and Vaithiyanathan (2009) believe this adoption of wireless changes the old way of thinking of how employees work in the workspace; they're no longer tied to their desks. "Wi-Fi radios are appearing not in just laptops but also in equipment as diverse as mobile phones, parking meters, security cameras and home entertainment systems" (Ravichandiran & Vaithiyanathan, 2009). The number of wireless devices and the demand for mobile computing is projected to continue to grow this decade, with wireless technologies becoming smarter, cheaper, and more secure (Ravichandiran & Vaithiyanathan, 2009). Wireless looks to become the model way of communicating in the years to come.

The problem right now is tied to funding. DoD organizations such as the Marine Corps are forced to be even better stewards of the taxpayers' dollars. Budget sequestration and other financial constraints are forcing the Marine Corps, an already financially limited organization, to be very selective and critical of every dollar spent. The idea of doing more with less is propagating throughout the Marine Corps and programs are being cut. Lawlor (2004) discusses how funding many programs has been challenging giving the numerous budget cuts and financial reductions that hit the DoD. As a result, clashes between current operations and programs and future ones are causing competing priorities of which only a fraction can be funded (Lawlor, 2004).

This thesis looked at some of the costs associated with acquiring a wireless capability in comparison to current wired COC capabilities and other available options. If money is not an issue in the future, a strong recommendation can be made to adopt a wireless solution that will enhance the flexibility and expandability of the Marine Corps. Even with a relaxed or flexible budget to adopt a wireless solution, one should be acquired at an affordable price with the understanding that there is potential for cost savings and other benefits that can result from going wireless. The reduction in manpower costs is probably not that big of a deal because that is already being done in the Marine Corps. In the short run, the adoption of a wireless solution without cutting the manpower that operates and maintains this technology will just be realigned and prioritized to other areas.

The COC CapSets were contracted in 2002 and a strong argument can be made that the technology is outdated. In the early 2000s wireless technologies were still fairly young in development and not as mature or secure as they are today. The backbone of most Marine communications' network infrastructures are capped in bandwidth and throughput of the weakest system in the transmission scheme so having a big and fast wired or wireless bandwidth or throughput pipe is really a moot point. The system will only go fast as it is capable, so in my opinion a lot of weight should not be focused on bandwidth and throughput size because both technologies are more than adequately capable. In Chapters II and III, the strengths and weaknesses of introducing a wireless networking capability to Marine Corps COCs were discussed. One advantage of the wired COC CapSet models is that the Marine Corps already have these systems and compatible devices and radios to work with them. An argument can be made that this has the potential to be a disadvantage if other organizations like the Navy and Army, are able to acquire or have newer technologies, which can have an effect on joint interoperability and efficiencies when hardware and capabilities of the current wired COC CapSet suites are not able to keep up. Security is always of issue, but an argument can be made that wireless technology on an unclassified network in a physically secure COC on a forward-operating base will have enough security controls to mitigate or negate the possibility of attacks from the outside. Inside attacks will be harder to defend against, but it would not

be any more difficult than that of a wired nature currently employed in the COC. The greatest benefit of wireless will be recognized when installing local area network connections such as those in the COC CapSets.

This thesis focused on the technology, financials, benefits, limitations, and opportunities of adopting a new wireless solution in the COC in comparison to what capabilities and technologies are already available and paid for. A critical requirement that the Marine Corps fleets desired to fulfill by adopting a wireless infrastructure over a wired COC infrastructure was to give the acquisitions personnel, communications planner, and any other decision maker of limited familiarity of wireless technologies, information needed in order to give them a general understanding of wireless technologies to aid them in making an informed wireless acquisitions decision. This thesis aims to serve as a quick guidebook that professional and/or novices in wireless and wired communications can reference.

Based on the analysis and research in this thesis an argument can be supported to continue operating the current wired COC CapSets because it allows the Marine Corps to eliminate any new costs and still affords the Marine Corps the technology and efficiencies it needs in order to stay effective on the battlefield. Although no new costs will be occurred in keeping current wired COC CapSets, the argument can be made that with the rapid adoption of wireless technologies by external organizations both commercial and government, the Marine Corps could quite possibly be missing out on some opportunities that would make COC operations more effective. A counter argument can be made that costs of these newer technologies will decrease significantly due to the saturation of wireless technologies on the market which will then allow the Marine Corps to take advantage of these technologies at lower prices.

One area of interest that would help advance this thesis is in the adoption and implementation of a secure wireless technology that would support both classified and unclassified networks and systems. The items in this thesis were of a general nature to not divulge any sensitive systems, operations, and/or information in order to keep this thesis unclassified. With the rapid advancement of information technology the need to update and expand on this thesis should also be looked at for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albert D., Garstka, J., & Stein, F. (2000). *Network Centric Warfare: Developing and leveraging information superiority 2nd edition.* Washington, DC: DoD C4iSR Cooperative Research Program.

Anthens, G. (2003). ROI Guide: *Payback period*. Retrieved from: http://www.computerworld.com/s/article/78529/ROI_Guide_Payback_Period.

Assistant Secretary of Defense. (2009). *Use of commercial wireless local area network (WLAN) devices, systems, and technologies in the department of defense (DoD)* global information grid (GIG). Washington, DC: Department of Defense.

Brain, M., Wilson, T., & Johnson, B. (2013). *How WiFi works.* Retrieved from: http://www.howstuffworks.com/wireless-network.htm).

Burkhart, C. (2004). *Where is my frequency?* Retrieved from: http://www.mca-marines.org/gazette/where_is_my_frequency.

Chiu, Y., Logman, H., Chiu, M., & Sunkara, A. (2005). *Guidebook for selecting cost-effective wireless communication technologies for intelligent transportation systems.* Retrieved from: http://www.utexas.edu/research/ctr/pdf_reports/0_4449_P1.pdf

Coleman, D., & Diener, N. (2007). *Protecting WiFi networks.* Retrieved from: https://www.cisco.com/en/U.S./prod/collateral/wireless/ps9391/ps9393/ps9394/prod_white_paper0900aecd807395b9.pdf

Coleman, D., & Westcott, D. (2012). *CWNA certified wireless network administrator official study guide* 3rd Edition. Indianapolis, IN: John Wiley and Sons, Inc.

Dhawan, S. (2007). *Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX*. (Master's thesis). Retrieved from IEEE Xplore Digital Library. doi:10.1109/AUSWIRELESS.2007.27.

Defense Industry Daily Staff. (2009). *$54M to general dynamics for USMC combat operations center replacements*. Retrieved from: http://www.defenseindustrydaily.com/54M-to-General-Dynamics-for-USMC-Combat-Operations-Center-Replacements-05993/

Federal Communications Commission. (2013). *Radio Spectrum Allocation.* Retrieved from: http://www.fcc.gov/encyclopedia/radio-spectrum-allocation.

Gast, M. (2005). *802.11 Wireless networks: The definitive guide*, 2nd Edition. Sebastopol, CA: O'Reilly Media, Inc.

Hurwitz, J., Bloor, R., Kaufman, M., & Halper, F. (2012) *Hybrid Cloud for Dummies.* Hoboken, NJ: John Wiley & Sons.

Institute of Electrical and Electronics Engineers. (2012). *IEEE standard for Ethernet.* New York, NY: The Institute of Electrical and Electronics Engineers, Inc.

Inside Defense.com. (2012). *DBB Recommends Defense Secretary Push for IT Reform, Create Clear Strategy.* 19 Jan 2012. Web. 26 Feb 2012.

Jean, G. (2010). *Marine Corps prepares for budget cuts and uncertain future.* Retrieved from: http://www.nationaldefensemagazine.org/archive/2010/June/Pages/MarineCorpsPreparesForBudgetCuts.aspx

Jindal, S., Jindal, A., Gupta, N. (2005). *Grouping WI-Max, 3G and WI-FI for wireless* broadband. Retrieved from: IEEE Xplore Digital Library. doi:0.1109/CANET.2005.1598202

Lawlor, M. (2004). *New Operations Centers Set the Stage for Consistent Technology Acquisition.* Retrieved from: http://www.afcea.org/content/?q=node/217

Mitchell, B. (2013). *WiMAX*. Retrieved from: http://compnetworking.about.com/od/wirelessinternet/g/bldef_wimax.htm

National Institute of Standards and Technology. (2013). *Computer security division: Computer security resource center*. Retrieved from: http://csrc.nist.gov/about/index.html

Office of the Secretary of the Navy Financial Management and Comptroller. (2013). *Highlights of the Department of the Navy FY 2014 Budget* [PDF document]. Retrieved from: http://www.finance.hq.navy.mil/FMB/14pres/Highlights_book.pdf

Office of Management and Budget (OMB). (2013). *2014 Department of Defense Budget.* Retrieved from: http://www.whitehouse.gov/sites/default/files/omb/budget/fy2014/assets/defense.pdf

O'Sullivan, J. (2001). *Potential vulnerabilities of a USMC tactical wireless local area network.* Retrieved from: accession number: ADA397268

Palmer, D. (2012). *What is Bluetooth*. Retrieved from: http://www.techradar.com/us/news/phone-and-communications/mobile-phones/what-is-bluetooth-1063913

Persistent Systems. (2013). *Technology*. Retrieved from: http://www.persistentsystems.com/technology.php

Phifer, L. (2011). Anatomy of a Wireless “Evil Twin” Attack (Part 1). Retrieved from: http://www.watchguard.com/infocenter/editorial/27061.asp.

PricewaterhouseCoopers (PwC). (2013). *Real time: The growing demand for data 2012 North America wireless industry survey.* Retrieved from: http://www.pwc.com/en_U.S./us/industry/communications/publications/assets/pwc-north-american-wireless-industy-survey-2012.pdf.

Rappaport, T.S. (2006). *Wireless Communications: Principles and practice*. Upper Saddle River, NJ: Prentice Hall.

Ravichandiran, C., & Vaithiyanathan, V. (2009). *An incisive SWOT analysis of Wi-Fi, wireless mesh, WiMAX, and mobile WiMAX technologies.* Retrieved from: IEEE Xplore Digital Library. doi: 10.1109/ICETC.2009.47.

Schwartz, M., & Abramson, N. (2009). *The Alohanet – surfing for wireless data [History of Communications]*. Retrieved from IEEE Xplore Digital Library. doi: 10.1109/MCOM.2009.5350363.

Shirey, R. (2000). *Network working group request for comments: 2828.* Retrieved from: http://www.ietf.org/rfc/rfc2828.txt

Stallings, W. (1998). *Cryptography and network security, Second Edition*. Upper Saddle River, NJ: Prentice Hall.

Stallings, W., Brown, L., & Howard, M. (2008). *Computer Security: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall.

Tilghman, A. (2013). *Hagel: Budget cuts will shrink pay, benefits and force*. Retrieved from: http://www.techradar.com/us/news/phone-and-communications/mobile-phones/what-is-bluetooth-1063913

United States Marine Corps (USMC). (2005). *TM 2000-OD/2C Principal technical characteristics of U.S. Marine Corps communications-electronics equipment*. Washington D.C: U.S. Marine Corps.

United States Marine Corps (USMC). (2007). *Marine Corps information assurance enterprise directive.* Washington, DC: U.S. Marine Corps.

United States Marine Corps (USMC). (2010). *MAGTF Communications Systems/ Marine Corps.* Washington, DC: Department of the Navy.

U.S. Department of Defense. (2012). Contract [Data file]. Retrieved from: http://www.defense.gov/contracts/contract.aspx?contractid=4818

U.S. Department of Defense. (2007). *Use of commercial wireless devices, services, and technologies in the department of defense global information grid.* Washington, DC: Department of Defense.

U.S. Department of Commerce.(2003).*United States Frequency Allocations: The radio spectrum.* Retrieved from: http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

Voelcker, J. (1986). *Helping computers communicate: The open systems interconnection model promises compatibility for a variety of computer systems, although not all its functions are defined.* Retrieved from: IEEE Xplore Digital Library. doi: 10.1109/MSPEC.1986.6371030.

Wald, H. (2010). *IA Newsletter Vol 13 NO 2 Spring: Cloud Computing for the Federal Community.* Herndon, VA.

Wild Packets. (n.d.) *802.11 and the OSI model.* Retrieved from: http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_packets/pprintable

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California